DOCUMENT RESUME

ED 392 336 HE 028 924

TITLE	Realizing the Potential of Information Resources: Information, Technology, and Services. Track 2: Policies and Standards.
INSTITUTION	CAUSE, Boulder, Colo.
PUB DATE	96
NOTE	64p.; In: Realizing the Potential of Information Resources: Information, Technology, and Services. Proceedings of the CAUSE Annual Conference (New Orleans, Louisiana, November 28-December 3, 1995); see HE 028 922.
AVAILABLE FROM	CAUSE Exchange Library, 4840 Pearl East Circle, Suite 302E, Boulder, CO 80303 (individual papers available to CAUSE members at cost of reproduction).
PUB TYPE	Reports - Descriptive (141) -- Speeches/Conference Papers (150)
EDRS PRICE	MF01/PC03 Plus Postage.
DESCRIPTORS	Access to Information; Colleges; *Computer Networks; *Computer Security; Computer Uses in Education; Educational Change; *Higher Education; *Information Management; *Information Services; Information Systems; Information Technology; Legal Problems; Outreach Programs; Privacy; *Standards; Universities
IDENTIFIERS	Catholic University of America DC; *CAUSE National Conference; Dallas Baptist University TX

ABSTRACT

Seven papers and one abstract of a paper are presented from the 1995 CAUSE conference track on policies and standards issues faced by managers of information technology at colleges and universities. The papers include: (1) "University/College Information System Structures and Policies: Do They Make a Difference? An Initial Assessment" (Bruce Rocheleau); (2) "An Outreach Effort--The Connections Program" (Ardoth A. Hassler and others), which discusses efforts by the Catholic University of America to establish a computer network with local high schools; (3) "The CWIS Is Dead! Long Live the CWIN!" (Cedric Bennett), which compares the Campus Wide Information System and Campus Wide Information Network models of information exchange; (4) "Secure Your Network in Ten Easy Steps" (Roger Safian), an abstract of a paper on network security; (5) "The 1990s Challenge of Insulating the Institution with 1980s Information Technology Policies" (Susan Stager and others), which examines security, privacy, and legal issues; (6) "Reinventing the Wheel: Sometimes It's the Right Thing" (M. Shane Putnam), which describes the effects of systems reengineering on organizational change at Dallas Baptist University (Texas); (7) "Computer Security: Questions to Ask...Questions that Need Answers" (Louise M. Schulden); and (8) "Lock the Door and Throw Away the Key?...If We Cannot Provide Access to Data, Why Collect It? (Richard Pickett II and Darlene Quackenbush). Some papers contain references. (MDM)

ED 392 336

TRACK 2

POLICIES AND STANDARDS

Coordinator: Charles R. Schomper

Realizing the Potential of Information Resources:

Information, Technology, and Services

Proceedings of the 1995 CAUSE Annual Conference

HE 028 924

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

☐ This document has been reproduced as received from the person or organization originating it.

☑ Minor changes have been made to improve reproduction quality.

• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

PERMISSION TO REPRODUCE THIS MATERIAL HAS BEEN GRANTED BY

CAUSE

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

BEST COPY AVAILABLE

University/College Information System Structures and Policies: Do They Make A Difference? An Initial Assessment

Bruce Rocheleau, Ph.D.
Northern Illinois University
DeKalb, IL 60115

ABSTRACT: There is a substantial amount of variation in college/university computing structures (e.g., whether the university leadership is consolidated under a chief information officer), computing policies (e.g., the extent to which cost recovery is used), and planning efforts (e.g., the extent to which formal plans are developed concerning information and related policies). Although these policies have been frequently discussed, there has been little systematic research concerning whether these structures and policies have any impact on outcomes such as the extent of access and use made of computing by faculty, staff, and students. This paper draws on the 1994 CAUSE survey to provide an initial assessment of these issues.

INTRODUCTION

Henry Lucas studied the power and prestige of information service departments in 1984 and found that they had little power and visibility in most organizations.[1] But computing is now becoming a central activity of strategic importance to both universities and businesses. For example, Mara points out that the definition of a user of information technology at Cornell has changed from a hundred or so central office users to over 20,000 members of the university community.[2] If colleges and universities are to attract and keep top notch staff, faculty, and students, they need to serve a full range of users and support the teaching, research, and administration needs of their institutions.

To achieve these goals, information managers in colleges and universities need to know what policies are effective. What measures can they take that will help ensure success? For example, in recent years, many universities have spent a great deal of time developing technology plans including strategic, telecommunication, networking, administrative, library, and academic components. Although plans may help to bring about enhanced effectiveness, there is skepticism about the utility of planning because many plans remain on shelves unused. Do universities that construct formal plans (e.g., for networking) have more successful results (e.g., higher percentage of their micros/workstations networked) than those who do not formally plan? Do plans that are updated annually or linked to the budget have more impact?

The Chief Information Officer (CIO) has become a familiar position in universities and colleges. Slightly more than 75 percent of the institutions in the 1994 CAUSE survey reported that there was a CIO, though only about 56 percent said that the CIO is recognized "as such" in their organization. CIOs may come under attack if they are not viewed as being effective. For example, a recent article asked the question, "Is Your CIO Adding Value?"[3] In the private sector, several CIOs have been fired and in the public sector, CIOs have recently become the lightning rods for controversy in several states as one former CIO noted:[4]

> States have to do more with less and they think that technology is going to pull a rabbit out of the hat for them.

University CIOs may come under similar pressure as the strategic importance of computing grows. A recent paper noted that the organizational rather than technological challenges have been most difficult and that there still is disagreement about whether centralized or decentralized structures work best in a university setting.[5] Pitkin studied the role of college/university CIOs and found that they differed from their business counterparts because they did not carry out some roles necessary to be an effective executive.[6] The structure and power of the college/university CIO job can vary greatly. For example, some CIOs (about 18 percent) report directly to the Chief Executive Officer (CEO) of their college or university. About 33 percent report to the Chief Administrative Officer, 19 percent to the Chief Financial Officer, and the remainder report to a variety of others. Does it matter whether there is a CIO or whom the CIO reports to? Is a CIO who reports directly to the CEO without any intervening layers of administration more effective? Does it make any difference as far as use of computers in the curriculum whether the head of Academic Computing reports to the CIO?

Finally, there has been controversy over what budget and cost recovery policies are most effective in encouraging use of computing by faculty, staff, and students. Thomas M. Schwen, head of Instruction Technology at Indiana University, stated that he was worried about a backlash when campus decision makers found that faculty only made use of a tiny fraction (e.g., 1 or 2 percent) of the capabilities of high-tech classrooms.[7] Do student fees and chargeback systems keep students and professors from using the Internet? There have been reports that high network costs have done so.[8] Similarly, do colleges/universities with ongoing budgets (about 35 percent of our sample) for replacing micros and workstations have faculty and students more involved with computing in the curriculum and the Internet? Which policies, if any, positively influence the spread of academic use of computers.

The above questions deserve attention and careful study involving a variety of approaches including case studies, and the employment of experimental and quasi-experimental designs. Our study is exploratory, aimed more at focusing attention on these issues and developing hypotheses than reaching final conclusions about these questions. But the importance of these issues cannot be underestimated. Many people argue that information technology has been slow to permeate the curriculum of colleges and universities. For example, Cotton found that the percentage of courses in which information technology was integrated into the curriculum was 17 percent, no higher than in their kindergarten to high school study.[9] Steger, Williams, McClure, and Smith recently pointed to the dearth of evaluation studies concerning technology expenditures and the need to conduct such evaluations due to the shrinking economic resources available to universities.[10] Can universities modify their policies and structure to improve outcomes? These are the issues that we wish to address here. These are important issues. We hope that this paper will help to stimulate research on this topic.

METHODS

We began this study with a series of case studies conducted during 1993 concerning the structure and role of information technology at five Midwestern colleges and universities. Interviews were conducted with a variety of information technology staff, and also faculty and administrators at each institution. These case studies led to the devlelopment of hypotheses that, with the permission and assistance of the CAUSE staff, we were able to explore through analysis of the 1994 CAUSE survey which contained several relevant questions.

Our CAUSE survey sample used in this paper excludes surveys from 2-year, specialized, and uncoded institutions and the total sample size was 296. The total response rate for the CAUSE survey was approximately 39 percent. There is no way to determine whether, or to what extent, the responding institutions are different from the institutions that did not respond to the survey so caution must be applied to generalizing beyond the respondents to the survey.

As shown in Figure 1 below, we studied four major categories of independent variables (Planning activities, CIO-Organizational Structure, Computer Charge Policies, and Resource Allocation Variables) concerning their impact on the outcome variables. A detailed list of variables employed in the analysis is provided in Figure 2.

Figure 1: Major Variable Groups Studied

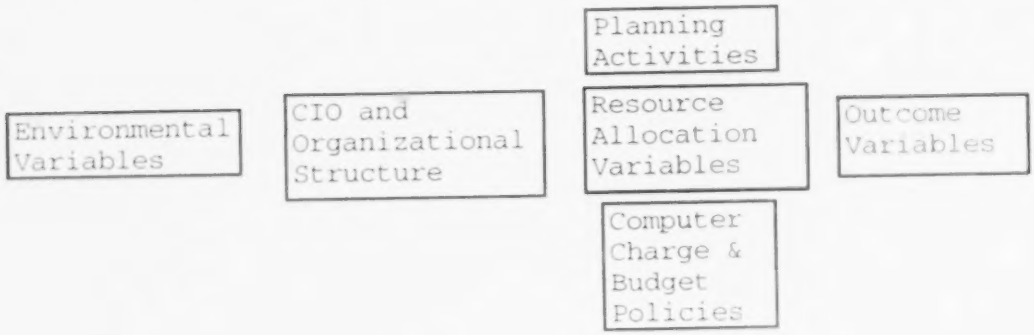


Figure 2
List of Variables Employed in Analysis

Planning Activities
- Institution has overall campus strategic plan
- Institution has IT Strategic Plan
- Is IT plan part of overall plan?
- IT Plan Covers Academic Computing
- IT Plan Covers Administrative Computing
- IT Plan Covers Telecommunications
- IT Plan Covers Library
- IT Plan Covers Networking
- IT Plan Linked to Budget
- IT Plan updated Regularly
- Composite Measure of Planning Activity (0 to 8)

CIO Power
- Is there a CIO?
- IS CIO recognized as such?
- CIO reports directly to CEO
- Academic Computing reports to CIO
- Administrative Computing reports to CIO
- Composite Measure of CIO power (0 to 5)

Computer Charge and Budget Policies
- Are there Student Fees?
- Chargeback (None, Partial, Full) for Academic Computing
- Chargeback (None, Partial, Full) for Administrative Computing
- Is there an ongoing budget for replacing micros/workstations?

Environmental Variables
- Public or Private institution?
- Type of Institution (Carnegie Class)
- Size of Institution (FTE's)
- Index of Resources (Ratio of micros/workstations to FTE's)

Resource Allocation Variables:
- Percent of Faculty with exclusive use of micro/workstati
- Ratio of micros/workstations to students
- Ratio of micros/workstations to faculty
- Ratio of micros/workstations to staff
- Does Institution provide access in dorms to micros?
- Percent of micros/workstations that are academic

Outcome Variables:
- Percent of Faculty making use of software in classroom
- Percent of Faculty making use of computing in curriculum
- Composite Index of Faculty having access to & Using Email, Gopher, & Web
- Composite Index of Staff having access to & using Email, Gopher, & Web
- Composite Index of Students having access to & using Email, Gopher, & Web
- Percent of Academic micros/workstations networked
- Percent of Administrative micros/workstations networked

Our analysis used a variety of statistical analyses including the use of a series of multiple regressions and partial correlation analyses. These techniques allow us to study the impact of several independent variables (the structures and policies of universities) on outcomes simultaneously while "holding constant" (statistically) the infuence of certain environmental variables such as the size of the institution and its resources. It is important to control for size because, for example, the larger universities have more resources that make it more likely that they will construct formal plans. Also, the general wealth of a university may allow it to look good on outcome measures though its plans and policies may not be especially effective. Although our index of resources was crude, examination of institutions high on this variable confirmed that many wealthy private universities scored among the leaders on this index (e.g., Harvard, University of Pennsylvania, Williams College, and Duke University) which supports our argument that this measure helps to control for institutional resources and wealth. We also studied the impact of other potentially relevant variables such as the Carnegie Classification of the institution.

The study has several limitations that mean that we need to view the results as exploratory including the following:

1) Many variables are undoubtedly rough estimates including many of our key dependent variables (e.g., what percent of the staff, faculty, and students have access to and use e-mail, gopher, and the worldwide web).

2) In some of our analyses, there are a substantial number of missing cases for several variables including some outcome measures.

3) Although our analysis examined a large number of potentially important factors, many important variables are undoubtedly missing, especially those measuring the quality of the planning efforts.

4) This is a cross-sectional study and we need longitudinal studies to test for causal relationships among the variables.

Despite these limitations, this study addresses significant issues and raises important questions for university officials seeking to discover what are the most effective policies.

PRESENTATION OF RESULTS

Table 1 summarizes our major findings. One fairly consistent predictor of outcomes was the presence of an ongoing budget for replacing micros/workstations. It was the only predictor of the percent of faculty use of computing in the curriculum and percent of administrative micros/workstations networked. It was also the best predictor of a composite measure of student access to email, gopher, and the Worldwide Web. An organizational structure in which Academic Computing reports to the CIO was the best predictor of the percent of academic micros/workstations networked and a composite measure of faculty and staff access to the Internet. It was the only predictor of the percent of faculty using software in the classroom. It should also be noted that the strength of the above predictors was quite modest, ranging from about 5 to 15 percent of the total variance (out of a possible 100 percent).

TABLE 1:
OUTCOME VARIABLES BY PREDICTORS (IN THEIR ORDER OF IMPORTANCE)[11]

Outcome #1: What percent of faculty make use of computing in the curriculum?
Predictor:
1) Institution has an ongoing budget for replacing micros/workstations.

Outcome #2: What percent of faculty makes use of software in the classroom?
Predictor:
1) Academic Computing Reports to the CIO.

Outcome #3: What percent of the academic micros/workstations are networked?
Predictors:
1) Academic Computing reports to CIO.
2) Institution has ongoing budget for replacement of micros/workstations.

Outcome #4: What percent of administrative micros/workstations are networked?
Predictor:
1) Institution has ongoing budget for replacement of micros/workstations.

Outcome #5: Composite Measure of Staff Access and Use of Email, Gopher, and Worldwide Web.
Predictors:
1. Academic Computing reports to the CIO.
2. There is an ongoing budget for replacing micros/workstations.
3. A composite measure of CIO power (Negative).
4. Institution is public.
5. CIO is recognized as such.

Outcome #6: Composite Measure of Student Access and Use of Email, Gopher, and Worldwide Web.
Predictors:
1. Institution has ongoing budget for replacement of micros/workstations.
2. Academic Computing is covered in the IT plan.

Outcome #7: Composite Measure of Faculty Access and Use of Email, Gopher, and Worldwide Web.
Predictors:
1. Academic Computing reports to the CIO.
2. There is an ongoing budget for replacing micros/workstations.

In the above analyses, we initially excluded the Resource Allocation variables because we wanted to focus on the impact of the structural and policy issues. When we added the Resource Allocation variables to the analysis such as Percent of Instructors with exclusive use of an institutional micro/workstation and student access to micros in their dorms, we were able to predict better the percent of faculty making use of software in the classroom and in the curriculum though the percent of variance explained still remained modest.

SUMMARY AND CONCLUSION

We did find some consistent results in our analysis. Generally, the existence of a plan was not a good predictor of outcomes. The existence of an academic plan did help somewhat to increase overall student access to the internet. But, the existence of IT plan that covered academics did not predict use of computing in the curriculum. Likewise, existence of a networking plan was not a predictor of the percent of micros/workstations networked. Neither updating of the plan nor linking it to the budget proved to be predictors in the above analyses.[12] The quality of the plan effort and the nature of the process may be crucial to plan success and we had no way of measuring these aspects of planning efforts. Institutions in which Academic Computing reports to the CIO were more likely to have superior outcomes. Other CIO-related variables were not important. The fact that the CIO reported directly to the CEO did not have any major positive impacts. The computer charge variables turned out to be generally unimportant--student fees had no statistically significant correlations with the student index of access to the Internet nor use in the classroom or curriculum. The environmental variables (FTEs, public or private institution, Carnegie Classification, and our index of resources) had modest relationships with most of the outcome measures.

To sum it up, our results were mixed. However, the significance of the ongoing budget and academic computing-CIO relationship suggests that budget and structural factors can have impact. Having a budget to replace micros/workstations is a very concrete activity and appears to have a beneficial impact on networking and use of computing in the curriculum. We checked and discovered that having an ongoing budget was not correlated with our measure of resources and wealth (ratio of micros/workstations to FTEs). Our results also suggest that a structure with CIOs in charge of academic computing has a positive impact on outcomes. As expectations concerning information technology continue to soar, colleges and universities need to put more effort into linking their scarce resources (such as time putting together plans) to bottomline results. Although many of the plans, structures and policies did not have much effect on outcomes, perhaps others (e.g., incentives for faculty to use computers) have more effect? Finally, the above research was done using 1994 CAUSE data. In the last year, there appears to have been a revolution in access to and use of the Internet. Has use of computing in the curriculum had a corresponding change? Can we identify any other policies that encourage good outcomes? We need answers to these questions.

NOTES

1. Henry C. Lucas, Jr. "Organizational Power and the Information Services Department," Communications of the ACM, January 1984, pp. 58-65.

2. Mark Mara, "Implementing Distributed Computing at Cornell University," Paper delivered at the 1993 CAUSE Conference, Boulder, Colorado: CAUSE.

3. Michael J. Earl and David F. Feeny. "IS Your CIO Adding Value?" Sloan Management Review, Spring 1994, pp. 11-20.

4. Tod Newcome, "The CIO - Lightning Rod for IT Troubles?" Government Technology, October 1995, p. 58.

5. Joseph J. Branin, George D'Elia, and Douglas Lund, "Integrating Information Services in an Academic Setting: The Organizational and Technical Challenge," CAUSE/EFFECT, Fall 1994.

6. Gary M. Pitkin, "Leadership and the Changing Role of the Chief Information Officer in Higher Education," Paper delivered at 1993 CAUSE Conference, Boulder, Colorado: CAUSE.

7. Thomas J. DeLoughry, "Colleges Told to Take 'Disciplined Approach to Technology,'" Chronicle of Higher Education, October 27, 1993, a22-a23.

8. See, for example, Thomas J. DeLoughry, "Unconnected: High Network Costs and Low Interest Keep Many Off the Internet," Chronicle of Higher Education, February 23, 1994, a19-a20.

9. Carole Cotton, "Talking Turkey About "Real Change,"" Paper Presented at the 1993 CAUSE Conference, Boulder, Colorado, CAUSE, p. 5.

10. Susan F. Stager, James G. Williams, Polley Ann McClure, and John W. Smith, "Assessing the Effectiveness of Information Technology," Paper delivered at the 1993 CAUSE Conference, Boulder, Colorado: CAUSE.

11. Note: The relationships are positive unless otherwise noted.

12. Note that we only present here the composite results for the impact on the use of email, gopher, and worldwide web. We did 18 individual analyses and in a few, the updating and linking of the plan to the budget, did appear as predictors.

BEST COPY AVAILABLE

An Outreach Effort - The Connections Program

Ardoth A. Hassler[1]
Executive Director, Academic Computing and
Information Technology and
CIO for the Main Campus
Georgetown University
Washington, D.C. 20057

Steven H. Chin
Assistant Dean
The School of Engineering
The Catholic University of America
Washington, D.C. 20064

Mary Jac M. Reed
Director of Academic Computing Services
and Acting Executive Director
Computer Center
The Catholic University of America
Washington, D.C. 20064

Abstract

The Catholic University of America (CUA) School of Engineering and Computer Center are in the process of connecting 15 local-area high schools to the existing campus network to provide Internet access in a project called "The Connections Program."[2] This paper will discuss the partnering experiences, describe the technology used, discuss the development of an affiliation agreement between CUA and the schools, and discuss the importance of developing acceptable use policies. These experiences should benefit other institutions undertaking similar projects.

---

[1] Ardoth A. Hassler is former Executive Director, Computer Center, The Catholic University of America.

[2] This work was supported in part by the National Science Foundation under NSF Grant NCR-9417569. The text of the grant is available online at http://www.cua.edu/www/ec_acs/project.

Introduction

There has been a downward trend in engineering enrollment over the past few years. In today's high-technology environment, introducing scientific and engineering concepts early in a student's educational experience is critical in fostering interest in technology. At the same time, an "information revolution" has occurred that requires educators of all levels and disciplines to constantly upgrade their skills. These factors contributed to the need for the Connections Program.

The Catholic University of America School of Engineering has a consortium with Washington, D.C.-area high schools. Through the consortium, many activities are being sponsored by CUA including Engineering 2000, Experiences in Engineering, Telecommunications 2000, Discover Engineering, and The Connections Program. The purpose of The Connections Program, funded by the National Science Foundation, is to expand the successful consortium activities to include providing computer technology to selected high schools in the Washington, D.C. area via a high-speed communication network.

Prior to the inception of The Connections Program, a few local high schools were connected via high-speed modems to a high-powered workstation server located within the School of Engineering. This workstation provides access to a variety of computational resources used in the engineering curriculum, as well as access to the worldwide Internet through the campus network. Funded in part by a grant from the National Science Foundation, The Connections Program extends this benefit to a larger number of high schools. When a high school is in the process of connecting, the School of Engineering provides network consulting expertise, assisting them in getting proper hardware and communications connections.

The Partnerships

The Connections Program would not have been possible without partnerships. From the beginning it has been a collaborative effort between the School of Engineering, the Computer Center, the high schools, vendors, and the National Science Foundation.

Existing Programs for the High Schools

The School of Engineering has an affiliation with the local high schools in the Washington, D.C. area whose goal is to stimulate interest in engineering among high school students. There are currently 14 participating high schools, many of which include a student population with high minority and female enrollments (two of the schools are all-girls). The Connections Program follows several initiatives sponsored by the School of Engineering, and was designed to complement them.

Engineering 2000

Engineering 2000 is presented as a one-week tour of the engineering concepts of the twenty-first century as seen by some of the most exciting of today's practitioners. The program includes a live-in, college-like experience and is intended to attract capable high school seniors to undergraduate engineering curricula. Attendance has grown from 80 (the target for the first year), to 160 (the maximum number CUA can handle with available facilities). The program draws students from all sections of the country, with a strong mix of female attendees (approximately 50%) and a core of black, Hispanic, and Native Americans.

Experiences in Engineering

Experiences in Engineering is a four-week, day program specifically targeting underrepresented minorities. This activity is sponsored jointly by the School of Engineering and the Society of Hispanic Professional Engineers, with partial financial support provided by NASA. Experiences in Engineering is intended to allow multiple-year attendance, up to three years. In addition to presenting an overview of engineering and the process of design, the program has an educational component for which CUA draws on experienced high-school teachers. Another critical component is the use of a high ratio of undergraduate students as teaching assistants to maximize hands-on activity and encourage mentoring. The targeted population is 25 students in each of the three years.

Discover Engineering

A three-hour evening program patterned as a "mini" Engineering 2000 is held specifically at the request of a high school at the CUA facilities. It provides an opportunity for a targeted group to visit the School of Engineering and meet with faculty and students and hear about programs available. This Open House activity is not restricted to the affiliated high schools.

Telecommunications 2000

This summer enrichment program provides a guided tour of the information superhighway and the many career opportunities in the telecommunications industry available to selected high school students. The program gives participants a diverse experience by providing seminars, hands-on laboratory work, and field trips to industry sites.

Computer Center and School of Engineering

Staff of the Computer Center and faculty of the School of Engineering worked together to design a relatively lowcost way to provide connectivity to the participating high schools. They have developed a plan for training faculty, network administrators, and students at the high schools. The result was a proposal that was submitted to and funded by the National Science Foundation. The final proposal and resulting grant were ones that neither group could have obtained on their own. Once the grant was awarded, work began on the building of a support system based on a DEC Alpha server and implementation of NT on servers, both funded by the grant. This involved systems programming staff from the Computer Center, the co-principal investigator in Engineering and two students in the School of Engineering. Originally, the Executive Director of the Computer Center and the Assistant Dean of Engineering served as co-principal investigators for the project. When the former took another job and left CUA, the Assistant Dean of Engineering and the Acting Executive Director of the Computer Center, who had formerly coordinated the training, became co-principal investigators.

Vendor Partnerships

In providing access to the School of Engineering's networked facilities via the Connections Program, the high schools are given access to sophisticated computing tools used in scientific and engineering disciplines, which can be incorporated into classroom activities and projects. Commercially-available packages in mathematics, such as Matlab by The MathWorks, Inc., and Mathematica by Wolfram, Corp., are two targeted applications. These software applications have gained widespread acceptance in the engineering community which thereby assures applicability in later engineering and science studies. A major component of The Connections Program is to provide expertise so that the high schools will be able to effectively integrate these packages into their curriculum. Both vendors have been supportive of the program by allowing their software licenses to be interpreted so that the high school students could use the software at no additional cost.

Another important partnership is with BBN Planet Southeast (formerly SURAnet), through which CUA receives its Internet connectivity. They have provided support to this project by considering the high school affiliates as one entity. Thus, CUA obtained one affiliate membership at a cost of $1,000 per year that covered all of the participating high schools. The project would not have been feasible had each individual high school been required to pay an affiliate membership. BBN Planet Southeast will also be providing training for the participants. This is discussed more fully later in the paper.

The High Schools

The participating high schools are expected to provide their own infrastructure in order to connect to CUA under The Connections Program. Expertise among the schools varies. Most use Intel-based MS-DOS/Windows equipment, however, one school uses Macintoshes. When

necessary, the co-PI in Engineering and his students provide technical assistance as the schools move to build local-area networks.

The National Science Foundation

In August 1994, CUA was awarded a grant from the National Science Foundation. It provides for equipment to be purchased for the high schools, the purchase of the DEC Alpha Workstation in Engineering, an expansion of CUA's backbone network to accommodate the school's connectivity, funds to hire graduate students to assist with the implementation, and some operating monies. As in-kind contributions, CUA upgraded its 56KB link to the Internet to T1 and made other enhancements to its backbone network.

The Technology Used .

The network architecture relies on the most up-to-date technology in order to achieve the necessary functionality. It consists of several workstations performing specific tasks. A Sun SpareStation, named "Goofy," is responsible for maintaining the yellow pages. The administration of databases that contain user ID's, passwords, group names and host names with their corresponding IP addresses is simplified using the yellow pages services. The configuration has one yellow pages server (Goofy) and each workstation is a yellow pages client.

A DECstation 5100, named "Pluto," is responsible for maintaining the file system. All disks on the system are Network File System (NFS) mounted. NFS mounted disks allow users to access files in different systems as if they were local. The Internet AlphaServer 1000 4/200, running under the DEC UNIX operating system, serves the applications, including Matlab and Mathematica, for The Connections Program.

In order to provide remote system maintenance from the network site to the high schools, a Pentium PC is used as a Windows NT Server. This PC will also be used as the Web Server for this project, which is envisioned as the main tool for collaborating on the project and disseminating the results. Other conferencing tools, only now becoming available, are also being investigated. One CISCO router is connected to a bank of sixteen V.34 modems that are accessible to the participating high schools. The other CISCO router provides connectivity to the CUA Computer Center, which allows access to other resources crucial to this project such as the Internet connection and the library catalog. A block diagram is shown in Figure 1.

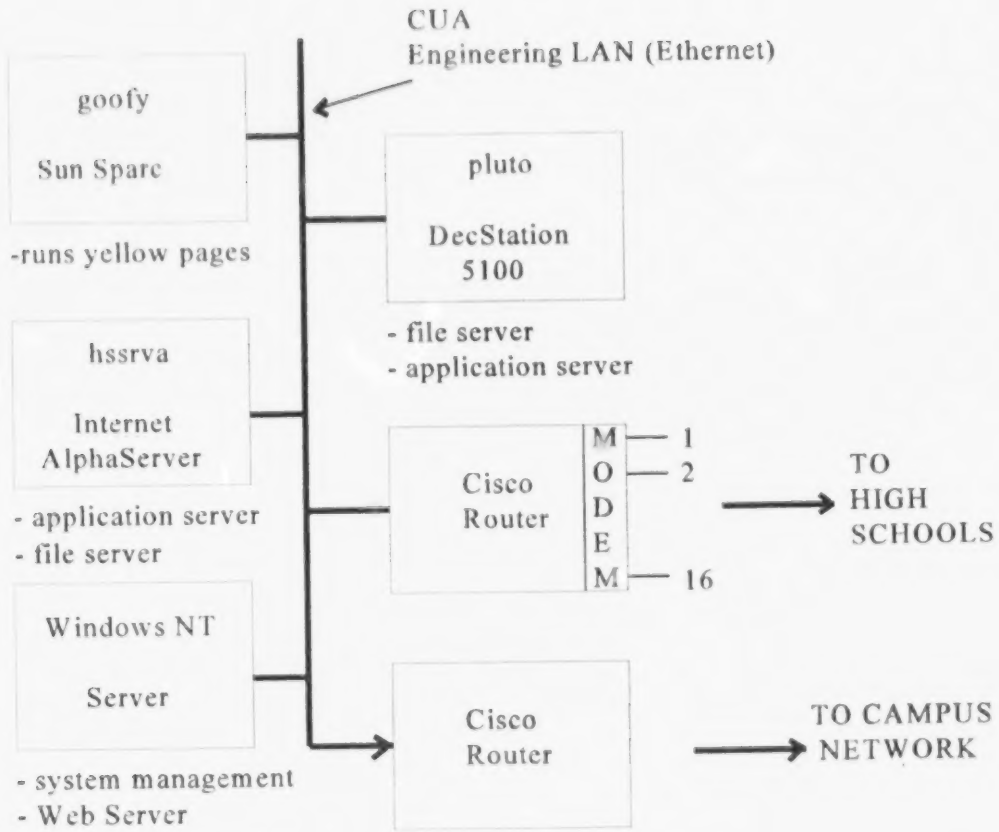


Figure 1 Network Architecture

Achieving Self Sufficiency

The participating high schools typically could not have assumed the total operating costs from the outset of the project. Thus, a transitional funding plan, depicted in Figure 2, was proposed and accepted by NSF. In it, NSF pays 100% of the operating costs the first year for telephone line charges and the membership fees to the Internet provider. The second year, the participating high schools are expected to assume one-third of the operating costs. They assume two-thirds of the operating costs in the third year. It was expected that three years would be sufficient for the schools to plan and budget these operating costs. Further, the schools were advised to plan and budget for the replacement of the equipment necessary to support the connections within five years of its original installation. This approach represents an increasing commitment by the high schools each year. It is envisioned that as they realize the benefits of the new technology, there will be no reluctance in maintaining their resources as well as assuming the full cost.

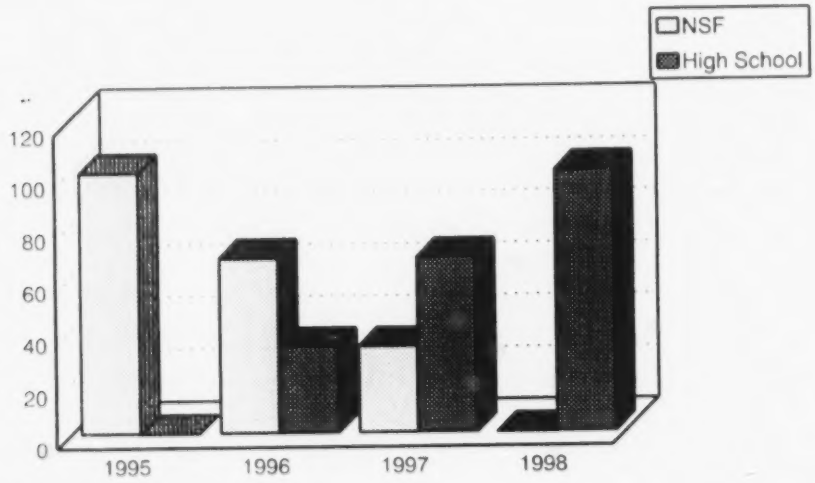


Figure 2 Cost Sharing

Training the Trainer

A key concept of this program, critical to the high schools obtaining self sufficiency, is to "train the trainer." A base of expertise must first be established at the high schools so that the tools available over the global Internet can be properly taught. A major investment must be made in "human capital" to ensure the success of this program. This is true for any initiative that relies on the participants keeping pace with technology.

Training is aimed at three target audiences: selected students, teachers, and network system administrators. A maximum of 15 students per session (two or three from each high school) are to be selected and given training on Internet resources at the introductory and

advanced levels. These students will act as mentors and guides to other students at their high schools, assisting other students in discovering the Internet resources. All teachers involved at each of the high schools will be trained at both the basic and advanced level of Internet resources. A training course specifically geared to network administrators as an introduction to networking basics will be offered and open to the designated network administrators from each of the participating high schools

The students and teachers will attend hands-on workshops provided by BBN Planet Southeast's staff members. The workshops are 1) Introduction to the Internet for K-12 Teachers and Librarians, 2) Introduction to Internet Technology for K-12 staff, and 3) Introduction to Internet Technology for K-12 Students.

The training seminars are offered throughout the year. Training is available to new participants and to continuing participants who are connecting to network resources at a more advanced level.

Responsibilities

An Affiliation Agreement was developed to define the partnering inherent in The Connections Program and to help assure that the schools were aware of not only their opportunities but their responsibilities. In the Affiliation Agreement, the duties and responsibilities of the university and the high schools are defined. The document serves as a written memorandum of understanding so there will be no misunderstandings of expectations by either party. A sample copy of the Affiliation Agreement has been submitted to the CAUSE Exchange Library and is also available on the World Wide Web at: http://www.cua.edu/www/cc_acs/project.

Among the items included in the Affiliation Agreement are a statement of CUA's hours of operation and when staff will be available should assistance be required with a connection. CUA currently staffs its computer operations area from 8A.M. to 12A.M., Monday through Friday. There was concern that the high schools would have the expectation of coverage and support 24 hours a day, seven days a week.

The Agreement further defines what software the students are permitted to use. The university was particularly sensitive about this as many of its license agreements restrict usage of software to current students, faculty and staff. It also stipulates that students are expected to use the facilities at their schools. They are not entitled to use the facilities on the CUA campus without explicit permission or invitation.

Each high school is made aware that the Internet is a compendium of computers and networks world wide that are linked together electronically and that there is no person or organization that coordinates or manages the Internet. The majority of these materials would be considered scholarly works; however, pornographic and other materials deemed unlawful and

unsuitable for anyone under 18 years of age are accessible over the Internet. The University cannot prevent a user from seeking out these materials. Although there is software commercially available that can "filter" unwanted material, it is certain that developers of unsuitable material will find ways to defeat these countermeasures. The Agreement states that the university will assume no responsibility for materials available on the Internet.

Acceptable Use Policies

An extremely important part of the Agreement from the university's perspective is that it spells out the high school's responsibility to educate students and their parents about responsible use of computers and networks. A sample statement of legal and ethical responsibilities is provided via the Affiliation Agreement to each high school participating in the program. There has recently been a flurry of activity in this area, as exemplified by numerous articles dedicated to this subject in the popular press. The schools are encouraged to tailor these materials or develop their own specific to their needs. Included is the suggestion that they obtain parental awareness of these issues for students participating in The Connections Program. One high school has already drafted a consent agreement that must be signed by each student *and* parent before access to the Internet via this project is permitted.

Summary/Conclusions

The Connections Program addresses a wide range of issues involving computer networking at the high schools. The implementation of the technology is an obvious consideration, but only one of many. The training being provided to designated high school teachers within the consortium on specific engineering software applications and on general knowledge and use of the Internet will hopefully work to enhance these benefits. Other equally important considerations are the investment of human capital, proper training, understanding the ethical issues involved in accessing the network, and a financial commitment to keep a modern networked computer facility--benefits obtained from the many partnerships inherent in this project.

The Connections Program is already promoting science and engineering in the secondary schools by extending the benefit of sophisticated computing resources to a larger number of schools and providing a much-needed educational tool. This project represents a modest beginning to what is a continuing effort in redefining the educational process in science and engineering. It is a given that use of these resources will soon extend to students and faculty in other disciplines.

The CWIS is Dead! Long Live the CWIN!

Cedric Bennett,
Director, Applications Support
Stanford University

Abstract

This paper compares two models for delivering wide, easy information-access for members of our institutional communities and beyond. It contrasts between centrally managed and supported systems and distributed networks and services. It uses this comparison as a means to explore several interesting management challenges which the deployment of these technologies have created, many of which are still to be addressed.

Newer information technologies support, and even encourage, widespread information sharing. Relatively easy-to-use protocols plus easy-to-obtain client and server code ported to a wide variety of platforms has made publishing information campus-wide, and even world-wide, a simple matter for anyone with a network connection and the will. These new technologies are replacing the notion of the Campus Wide Information System (with its implied central control) with the much more managerially complex concept of a Campus Wide Information Network (CWIN).

The CWIS is Dead! Long Live the CWIN!

Cedric Bennett,
Director, Applications Support
Stanford University

Where did the CWIS come from?

Providing Information

During the 1980's, many institutions sought ways to use information technologies to electronically share information widely across their campuses. For the most part, these technologies involved maintaining central information stores on large centrally managed processors, creating a mechanism for navigating to and through the information, and making it available to students, faculty and staff via terminal access. Management and process infrastructures were created (often using existing structures) to support the growth and maintenance of these information stores.

The types of information provided via these means were of various types – central policies and procedures, library catalog and other bibliographic data, instruction and documentation regarding electronic services themselves. In addition, they often had one major characteristic in common; the information providers were most often central organizations supplying information to other central and de-central organizations as well as to individuals.

These systems met the goals initially set for them of providing information from central information providers to central and de-central information consumers. However, for the most part they were expensive to establish and to maintain. Only a relatively few institutions actually provided such services. These systems eventually became known as Campus Wide Information Systems (CWIS).

Exchanging Information

During the same time period, other information exchange technologies were also becoming more and more available. NetNews, Bulletin Boards, and List Serves were gaining in popularity, at least among the technical community. These mechanisms were designed more for the exchange of information across the network and between colleagues than just information providers supplying information to information consumers – they provided a means for dialog not usually present in the other model. These technologies remained relatively difficult to use and did not spread dramatically beyond the technology community.

What's a CWIN?

Newer CWIS Technologies

At the close of the 1980's, newer, network-based, desktop-centric, 'point-and-click' technologies began to appear. These newer technologies supported and even encouraged widespread information sharing. Gopher[1] and World Wide Web (WWW)[2] protocols plus easy-to-obtain client and server code ported to a wide variety of platforms have made publishing information campus-wide, and even world-wide, a simple matter for anyone with a network connection and the will. In fact, it has been the acceptance and deployment of these technologies which has lead to the term "Campus Wide Information System" (CWIS).

All of a sudden, the means to provide information widely was within the grasp of any institution. Although Gopher began as the preferred approach, it was overtaken within a very few years by the WWW protocol — primarily because it is a faster growing, 'richer' protocol and because clients were created early that supported all popular systems.[3] The rapid acceptance of the "Web" both in academia and in the commercial world has created opportunities and it has exposed (or exacerbated) problems.

Campus Wide Information Network (CWIN)

Since it is true that anyone with the will to do so, can create a presence on the Web and can link that presence to any other presence on the Web, it is no longer appropriate to think in terms of just a "system" (which includes an implied concept of control). The Web is not as controllable an environment as the initial concepts and implementations of the CWIS. It requires a shift in thinking to understand that older system-oriented management principles will not work in such a widely distributed and networked information environment. For many providers, especially those already used to the CWIS idea, there is discomfort in the notion that information can be made so readily available.

Management Issues

Seekers, Providers, and Managers

The information environment has three principle players;

- those who are seeking information
- those who are providing information
- those who manage the information technology infrastructure

These roles have always existed, but have not always been clearly delineated (because providers and managers were often the same people or organization). Of course, it is possible that any single person or organization can play any or all of these roles. It is important to understand the similarities and differences of each.

---

[1] Originally developed at the University of Minnesota.
[2] Originally developed a CERN (The European Laboratory for Particle Physics in Switzerland).
[3] GUI clients, notably Mosaic from NCSA, were developed early for Unix, Windows, and Macintosh.

For seekers of information, it is important that the mechanisms for seeking be easy to use (especially for inexperienced seekers). It is also important that the mechanisms be fast and allow experienced seekers to get to the sought after information in very direct ways. It is very important to all seekers that the information, once found, be known to be authoritative.[4]

For providers of information, it is important that the information being shared is easy to find. It is also important that the information be easy to maintain directly by the provider and not through some intermediary (i.e., to change, to withdraw, to create). And it is important to most providers that the authority level of the information be clear and believable.

For managers, there are many concerns; here are a few:

Usage Includes issues of living with the 'ad hoc' nature of the CWIN and satisfying the needs for authenticating the authority level of the information. It also includes server, network, and client performance issues.

Cost The tradeoffs of using open, public protocols vs. proprietary approaches and the ability to fully utilize work already done by others (make vs. buy vs. share vs. assemble).

Stewardship Who, at the institution, is responsible for "Home Page," the "look and feel' of the institutional pages, and the "protection" of the institution from inappropriate use (e.g., copyright compliance, what's official university information, unacceptable publication).

Support Who provides Web services to others? How are users (both seekers and providers) supported?

Information Policies What is the institution's electronic information policy? Who polices that policy?

Wrap up

The point of this article is simply to raise the idea that working with newer, network-based, information exchange technologies is going to require a new way of thinking and a new way of managing – perhaps best summed up in the phrase "managed anarchy." The notions and management principles that derive from a fully centralized systems point-of-view will not serve us well in this newer, distributed environment. That does not mean that we must give up all hope of management and even control of some aspects of the environment but only that it will require some additional thinking.

---

[4] More accurately, it is important that the authority level of the found information be clear (even information with little authority can be valuable – but its authority must be known.).

It is also useful to keep in mind that it is difficult to tell where this technology will eventually take us and what its impacts will be. We can be very sure that it will have an impact and that it will eventually be profound. It is much less certain just what those impacts will be.[5]

[5] The National Highway System got its start when Congress asked General Pershing to organize a system of National Defense Highways (which led to the publication of the so-called "Pershing Map" in 1922). No one at the time was able to predict the eventual impact on our society of a National Highway System. It is just as unlikely that we, at this time, can predict the eventual impact on our society of a National Information Infrastructure ("Information Highway").

Secure Your Network in Ten Easy Steps

Roger Safian
Network Security Coordinator,
Northwestern University

Abstract

This paper provides an overview of ten important considerations as we ponder how to make our campus networks more secure. Readers will find ideas they can implement immediately to improve the security of their networks.

Computer networks have become valuable tools. We have gone from a few centrally managed resources to hundreds and thousands of machines on our local networks. Yet, the very ease and proliferation of computer resources have brought about new and unforeseen consequences. We've all heard the stories. We've read about the hackers and crackers.

The ten points discussed are: policies, network design, your vendor, your O.S., passwords, organization, openness, security officer, law enforcement, vigilance.

Paper Not Available

The 1990s Challenge of Insulating the Institution with 1980s Information Technology Policies

Susan Stager, Ph.D., Indiana University
Virginia Rezmierski, Ph.D., University of Michigan
Tad Pinkerton, Ph.D., University of Wisconsin

The following document is a snapshot of the current policy environment at universities and colleges, the issues that are arising and are being debated. Many universities that have put policies in place to guide community functioning, are reviewing those policies to ensure that they are sufficiently robust to meet the challenges of the fast expanding and changing technology. While review of old policies is going on, new policy areas are also being identified and analyzed. New issues arise, partly analyzed issues continue to be discussed, partly approved policies wind their way through processes, and old policies continue to be in need of review. All exist within campus communities at the same time. Some policy issues even become obsolete before they go to press.

The 1990s Challenge of Insulating the Institution with 1980s Information Technology Policies

Susan Stager, Ph.D., Indiana University
Virginia Rezmierski, Ph.D., University of Michigan
Tad Pinkerton, Ph.D., University of Wisconsin

Introduction

Rushed to the implementation stage in the 1980s, IT computer use and security policies may appear flat, stilted, and superficial. The principles upon which these policies were built are still keys ones, however, and the appropriate foundation for policies in the 1990s. What requires interpretation is such cosmetic phrases in these policies as "computing resources should be used in accordance with the high ethical standards of the university community." What does this and similar phrases mean in the 1990s?

As this paper is being written, we await the fate of the Cox-Wyden Amendment to the telecommunications deregulation bill. The amendment forbids the FCC from regulating Internet content. It also provides some liability protection for Internet service providers like colleges and universities if a good faith effort is made to prevent distribution of obscene material. This amendment symbolizes the moving target of legal and ethical solutions to problems encountered by colleges and universities as they provide Internet service to their campus community. One moment we think we have a clear reading on Congressional intent, the next moment a new amendment is introduced.

The following document is a snapshot of the current policy environment at universities and colleges, the issues that are arising and are being debated. Many universities that have put policies in place to guide community functioning, are reviewing those policies to ensure that they are sufficiently robust to meet the challenges of the fast expanding and changing technology. While review of old policies is going on, new policy areas are also being identified and analyzed. New issues arise, partly analyzed issues continue to be discussed, partly approved policies wind their way through processes, and old policies continue to be in need of

review. All exist within campus communities at the same time. Some policy issues even become obsolete before they go to press.

I. Historical--Yet Still Around--Policy Issues

There are policy issues that we have faced in the past which continue to need attention on university and college campuses. The following section identifies some of those issues.

A. Harassment

The populations of universities and colleges are made up of a high percentage of young adults. Many are experimenting with and/or refining new ways of communicating with their peers and with others. Technological changes cause all of us, regardless of age, to learn new ways of using the technology to get our messages across to others. In this fast changing arena we all respond at times without thinking carefully about the impact of our words. We all struggle with how to enhance our messages with the nonverbal cues that we use so readily in our face-to-face communications. We all need to be aware of, and responsive to, the personal boundaries of others and when and how we may violate those boundaries during communication.

Harassment, insults, hurtful, insensitive language, are all found in everyday communication. What is new, is the speed with which we can pass such forms of language to many individuals, and do so with anonymity in some cases. What are the new forms of problematic communication that we see on campuses as information technology is used? What constitutes civil communication? When and how are boundaries crossed in interpersonal communications? When is a message a harassment? All of these issues need to be examined and community values regarding interpersonal communication strengthened on a continual basis within university and college communities.

B. Pornography

IT policy makers still struggle with the question of what is pornographic. Community standards within the ivory tower differ from those without. IT policy makers should watch other media -- newspapers, film, video,

cable, TV -- for trends. For example, a recent issue of EDUCOM Review reports that Time Warner Cable wants to "scramble" sexually explicit programs on its New York community access channel, and make subscribers request programs in writing. The ACLU has charged "censorship." Time Warner countered that it has the same right to control what it sends across the wires as the newspaper has to control what it prints. What control does IT have over its wires?

C. Copyright

Many students come from an environment in which copying music and videos is the norm. Many students believe that they are 'authorized' to copy any material that they require for their academic work. They equate student status with a special class of citizenry that can use information resources without cost.

The typical computer use policy contains a catch-all phrase with wording like the following: "Computing resources may not be used for illegal purposes. Examples of illegal purposes include: Unauthorized copying of copyrighted material." The student is no wiser after reading the statement than before.

The copyright issue is no less murky from within the walls of the computer center than outside. Copyright laws may protect program text, but it does not protect industrial design elements of the programs, such as command hierarchy in the Lotus v. Borland, case or the internal interfaces involved in the Altai v. Computer Associates case. (Communications of the ACM 1995) Copyright issues will continue to need attention and study.

D. E-Mail Privacy

Electronic communications are sweeping the campuses as the primary use of the technology. Electronic mail is used for interpersonal social communications, for the scheduling of meetings, for informal discussions of topics between staff, for discussion of highly sensitive and personal topics, for generally open and free discussions of public topics, and for decision-making at some levels. Most disturbing is the fact that like most forms of communication there is a mix of several of the above content

types within many messages. Individuals use the tool to accomplish a number of objectives at one time.

Some of the communications that travel across electronic mail are strictly business related; many are not. Some institutions have provided electronic communication tools explicitly for the purpose of increasing open communication and discussion, for increasing the exercise of Freedom of Speech, for creation and play with ideas, and for increasing the intimacy of groups. Some have provided electronic communication tools explicitly, and perhaps solely, for business functions.

The law is unclear as to the privacy of electronic communications. Should universities and colleges monitor the use employees make of electronic mail? If someone complains about a message received by an employee, does the employer have the obligation, the right, to intercept and read communications? As we keep records of the amount of use of systems like electronic mail, is there information in those logs that could be analyzed to identify the amount of time individuals spend in use of e-mail or even the specific individuals with whom they communicates?

II. Current Policy Issues Gaining More Attention

A. Social Security Numbers as Common Identifiers In this section we identify those issues which are currently being debated because they have taken new form through the use of technology.

Periodically, the issue of a single card/number which will identify individuals, a common identifier, arises. Over the years, often from the initiation of an effort such as in the case of social security numbers, leaders initiating the effort have insisted that the number will not be used for purposes other than that originally intended. However, in each case, once established, the number/device becomes embedded and found to be useful for many other purposes; it is readily adapted and reused.

Will universities and colleges face legal action from those who wish to protect their financial and other personal information, as uses of social security number continues to proliferate? Will a unique number be used on

college campuses, one that is not tied so directly to personal financial and credit information? Or will the increasing use of debit cards on the campuses cause the use of identification cards, cards tied to social security number and other personal information, to expand well beyond what is currently imagined? Will the momentum and ease of the technological applications using these common numbers, overshadow the privacy concerns in the use of common identifiers?

B. Liability for E-mail Campus Directories v. Paper Campus Directories
Suffice it to say that many universities now have a process in place whereby a student, faculty, or staff member may have an "unlisted" e-mail address, comparable to an unlisted telephone number. Are campuses giving individuals choices in this regard? Are they allowing privacy in large national and international arenas, but public information in local arenas if that is desired by the student, staff, or faculty member? Or are system applications designed in such a way as to be automated without user choice, or to be inflexible to different needs at different levels of information dissemination? What are the liabilities as we handle this type of personal information--directory information?

C. E-mail Stalking
The crime of stalking received national attention several years ago because of a few celebrated cases, especially that of David Letterman. The crime of stalking has found new expression on the campus network. One university has had a case in which the activity of a computing-intensive female student was monitored by a male via VMS software listing the terminal of logged-on users. No physical contact was made between the stalker and the female, a condition of most stalker statutes currently enforced. But the motivation of the individual was the same as that of the traditional stalker, and the police acted.

D. E-mail Bombs--Box Stuffing
Minimal programming skills are necessary to create a program that will generate enough junk mail to flood a mail box and shut it down. Is it a form of harassment, a harmless prank, an act of vandalism, a problem with impulse control, an educational problem, or a serious threat to system security that one user can close down access, for another, purposefully? What does the university or college say to users about

equity of access, about reliability of access? What is university responsibility in this regard?

E. E-mail As the Core of Lawsuits

Thanks to Newsweek, Time, and other popular media, the public now recognizes that a deleted mail message isn't necessarily an unrecoverable piece of evidence. The critical piece of evidence in a lawsuit may be an e-mail message retrieved by a university staff member from a server or back-up tape. The absence of a message on a back-up tape can be just as useful to a case.

In the commercial world, computer system detectives are hired to search for discarded files and messages, or even reformatted hard disks. To what lengths should computer center staff go to retrieve data to assist university legal counsel or local law enforcement officials? How much staff time should be devoted to the task? What should users be told about back-up files and other storage media? What is available under the Freedom of Information Act, even if it is not sought through court order? Can we maintain electronic mail privacy for users? How important is it?

F. Political Activism Using the Campus Computer Resources

At one university, the fine line between politics and Free Speech on the campus network first became apparent when the electoral board fined one of the student political parties for using e-mail communications during the student presidential race. The next volley was fired during the city/county elections when a faculty used a distribution list to send an endorsement of candidates to his friends on campus. The next step was a request from a state representative to have a home page on the University system. Each step of the way there was debate about the proper role of the University.

Another form of political activism that may affect universities is of the "Tiannamein Square" variety. Students may involve the computer network in their struggles with administrators. While in the 1970s students brought universities to their knees by flushing all of the dorm toilets simultaneously, students could easily bring the campus computer system to its knees as well. When 4,000 people attempted to log into Goodard Space Flight Center to see comet Shoemaker-Levy hit Jupiter in 1994, the

system, designed for 30 simultaneous users, crashed. Campuses are already feeling the strain of scaling up to the number of simultaneous users that want to use the increasingly popular tools. Campus networks can crash with, or without, a political motivation.

III. Emerging Policy and Debate Issues

New issues arise almost daily as technology is being applied in new and modified ways. The issues identified in this section are just beginning to be debated on university and college campuses. Few policies are in place to guide communities in these areas as yet.

A. Digital Signatures

In the not-too-distant future, we will be amazed that we ever debated the validity of on-line signatures. In the Middle Ages it was necessary that heated wax, in the form of a symbol, be affixed to a document. The symbol might be the family seal embellished with mottoes. Today, our legal system finds that a promise can be binding without a written signature. Those of us who have performed the bulk of our work electronically for some years now, daily use our plain-text ASCII name in the e-mail "from" line as a symbol of our promise. And as time passes, we are more and more comfortable handling major business transactions with digital signatures. This society long ago dispensed with the seal as a sign that a promise would be enforced. Are we building adequate devices to ensure that a signature is what we believe it to be, and made by whom we expect?

B. Racial Electronic Terrorism

In October of 1994 someone broke into the computer account of a Texas professor and sent racist messages to about 20,000 computer users in four states. In response, about 500 users sent the professor death threats and other harsh responses.

Messages, felt to be racist or otherwise threatening and obnoxious, can be sent, responded to, forwarded, and many times duplicated without ever confirming the source of the original message, without identifying the actual sender. What is the role of education on campuses in these matters? What do we need to do to develop systems that help individuals confirm identities of senders of messages, or at least understand when

forged mail is received? What role, if any, do universities and colleges have in protecting their users from such acts of indirect terrorism?

C. Commercial Ventures on the Internet

With over 700 electronic malls and specialty stores on the Internet, all accessible from your campus computing network, it is difficult to enforce a campus policy of "no commercial use of the campus network." What is the purpose for which the campus network was created? Is it important to justify the use of the funds and try to restrict the commercial use of the network? Is expansion of the use of the campus network to non-affiliated users a natural, extension of service, solely driven by the potential of a new source of funds, or a needed extension of service to wider communities? Or is it a misuse of funds and an inappropriate intrusion into the life of the campus?

D. Authoritative Source for On-line Documents

With the immense popularity of the World Wide Web, and the desire of so many users to display documents in that environment, a significant question regarding representation comes into focus. What documents on the WWW represent the University? How does an institution confirm the validity and integrity of documents that purport to represent the University? What is the authoritative source for information? How does the institution organize and manage the input and updating of significant documents that represent their campus?

E. Institutional Records in the Electronic Environment

As administrators, faculty, and staff of universities and colleges create more and more documents within the electronic environment, and store them in different forms, identifying and preserving records becomes an important policy consideration. Who creates records? In what format or medium should records be created? If they are contained within electronic communications, how can record and non-record content be separated? How can the institution guarantee that documents that are created electronically, and perhaps stored electronically, will be available one year from now when, perhaps, systems are changed and information is transferred from place to place? How will the institution guarantee that the documents will be readable one year from now when, perhaps, the tools have been upgraded or discontinued? What should the operational

policy be within universities and colleges to ensure the creation, maintenance, and preservation of university records?

F. Handling of Personal Information

We are now able to pass information around the electronic environment of our institutions with increasing ease. Everyday it becomes easier to cross over the barriers caused by different technological platforms, and pass documents from one user to another. Administrators at many universities and colleges are talking about sending data between institutions over the networks. As each college and university faces these new potentials, they will need to examine the current and future practices when it comes to the handling of the personal information of members of their communities.

What is personal information? Is the newly digitized signature of an individual user the property of the University or of the individual? Can it be used in one or more ways? Did the individual understand the ramifications of giving that signature to be digitized? What about photographs? How can they be used by institutions? Do individuals understand the ways in which the University intends to use the photograph at the time that it is taken? Does the University even understand its own intent as it asks for this personal information? What will the universities and colleges do as they consider the possibility of transporting student grades, transcripts and other information between institutions? What policies will guide these decisions?

G. Image Alteration

Images are now possible to alter digitally without a trace. Photographs can so easily be changed that their use in court is being diminished. Soon we will be able to alter active video as well. What ramifications will this ability to alter images have on the campuses? Will altered images of a President of a University, for instance, be seen as Freedom of Expression or as character assassination? Will placing an individual in a scene falsely and publishing that picture be understood as misrepresentation, or artistic creativity? What are the policies and guidelines that will be needed to protect against impulsive administrative actions, and what will be needed to protect essential Liberties?

H. Libel Revisited

Colleges and universities remain uncertain as to their vulnerability for postings by students. An agreement was reached this month between the law firms representing Prodigy on-line services and Stratton Oakmont. Stratton Oakmont, an investment firm, felt it had been libeled on Prodigy when a user posted a message accusing the firm of "criminal fraud." In the agreement, Prodigy would not be held libel.

Hopefully this court decision will be generalized and put an end to concern that the university will be held responsible for postings on its computer network. In a sense, this court decision grants the computing network the same status as the telephone network in that telephone companies cannot be sued for libelous calls made on its lines.

IV. Enduring Principles in Current Policies

While the issues are complex and ever-arising, there are some enduring principles which seem to be repeated as we continue to debate old issues, participate in the current discussions, and examine the new emerging issues. These principles help to clarify issues as belonging to various continuation of values on campuses. Once we are able to identify what the issues are really about, it becomes easier to accomplish the values clarification work that must be part of any policy development process. Below are some of the enduring principles.

A. Distinguishing Between Private v. Public Information

The debate between public vs private information is being played out at all levels. Historically, many documents have been made available to the public at selected sites, such as libraries, requiring the public to come to that site in order to access the documents. With the growth of the superhighway, at the state and federal government levels, statutes, administrative codes, and the text of bills being considered by the legislature (including the bill's status and what its fiscal impact would be) are being made available over the Internet. Some states, such as New York, sell the information to provide another revenue source for government. California is on the other end of the spectrum, making the information available at no charge to anyone who wants it.

At the University level, debate reigns about what is public and what is private information. State and federal statutes take some of the guess work away. However, there is still a gray area. To further complicate the matter, statutes often use the terminology that public documents must be made 'accessible' to citizens. What does 'accessible' mean in the age of the Internet? Distinguishing between public and private information is a principle that will assist policy development.

B. Distinguishing Between Security and Ease of Use
The gap is widening between security on administrative computing systems and academic computing systems. At the same university, administrators may be required to transgress through three levels of passwords to acquire a database that is ultimately part of the same campus network used by students who routinely share their password with friends. Distinguishing between areas requiring security and those requiring ease of use is a principle that will benefit policy makers.

C. Distinguishing Between Institutional and Individual Ownership
The copyright laws are currently under revision, leaving the University in limbo on these critical issues. The complexity of copyright increases in the multimedia environment. The person who created the original work owns the copyright. Accordingly, the text might belong to the professor and the image might belong to the graphic artist. Yet in may institutions, the University owns the copyright for both because it employs both the professor and the graphic artist. Distinguishing between institutional and individual ownership in policy will provide guidance for communities.

D. Distinguishing Between Social Responsibility and Experimentation
Universities and colleges have a large investment in allowing free experimentation and creative expression on their campuses. Freedom of Speech is an imperative if we are to meet our missions of teaching, learning, and the creation of knowledge. But where does experimentation end and social harm begin? In this new electronic environment, how do we clarify the limits and boundaries of these concepts? Distinguishing between responsibility and experimentation and the limits of each, is an important principle for both policy making and for education.

Conclusion

The members of this panel have years of experience at their respective universities in contemplating the issues surrounding the use of information technology. They do not claim to have the answers to all of the questions raised in this paper or to those that will be raised during the panel presentation. However, they will share their thinking and the guiding principles that have helped them to cope with new issues. They will share advice as to how to deal with this exciting time for policy makers. They will look at 1990s challenges and the robustness of the 1980s policies that they have helped to create.

REINVENTING THE WHEEL:
Sometimes It's the Right Thing

M. Shane Putman
Sr. Analyst / Adjunct Professor of Business
Dallas Baptist University

ABSTRACT

This paper provides a detailed description of how Dallas Baptist University has used the impetus generated from implementing a new integrated campus administrative computer system to document, analyze, and recommend significant organizational changes. The changes were undertaken to improve overall campus efficiency and quality of service. The basis of the paper is the methods by which DBU reengineered major service processes on a campuswide scale. Illustrative examples include reengineered processes that were improved by as much as 200 percent.

In addition to discussion of the reengineering process, attention is drawn to actual case examples, documentation, and recommendations. Also addressed is the political skirmishes involved in the reengineering efforts, along with the techniques for overcoming resistance to the recommended restructuring.

The entire presentation has been created to help move reengineering efforts from a pie-in-the-sky conceptual plane to a truly practical, applicable level. The increased competition, shrinking budgets, and technological pressures of today's educational environment assure that this topic will be appropriate for some time to come.

"There is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success, than to take the lead in the introduction of a new order of things."
-- Niccolo Machiavelli, 1532

In the beginning, there were the Dark Ages. The technological infrastructure was formless and void, and Computing Services brooded over the chaos. The creators of the chaos were many and powerful. Fragmentation and replication of effort ruled individual departments. In an attempt to stem the tide, quasi-functional homegrown administrative software applications were poorly designed, poorly developed, poorly implemented, and were now impossible to maintain. Integration among the various software entities was sporadic, unworthy of trust, and a fond wish for the future. The two primary native populations -- faculty and administration - had founded the entire race relations on the foundation of noncommunication and mutual distrust.

While somewhat frivolous, the fictional account above includes far too many elements of truth. Dallas Baptist University had found itself on the horns of the same dilemma facing all institutions of higher education today -- how do we continue to provide a quality service and product to our students in the face of shrinking resources?

Dallas Baptist is a four-year liberal arts institution offering multiple degrees to the Master's level. We have an FTE of approximately 1,800 and a total enrollment of 3,100. However, unlike many institutions, nontraditional adults comprise a majority (53%) of our student population. The institution has found great success in partnering with working adults to allow them to complete a college degree either through our traditional undergrad programs or our experiential learning College of Adult Education. For students wishing to complete a graduate degree, we have partnership programs with many large corporations in the Dallas area including MCI, GTE, General Motors, and others to bring our educational resources to their sites. With several companies we have created lock-step MBA programs where groups of students are taken through our MBA program in a highly regimented, step-by-step curriculum from beginning to end. We have made great efforts to tailor our program to our demanding students' needs.

However, the implementation and effective continuation of such programs requires an incredible amount of flexibility and oversight, from faculty, staff, and administrative software systems. As time progressed and demands on our computing infrastructure increased, it became glaringly apparent the list of identified dysfunctionalities was growing rapidly, and the tools we had in place were failing to support our day-to-day business requirements, and were hopelessly unsuitable to support future growth strategies.

After upgrading the physical infrastructure of the campus computing environment, the next issues to address were the fragmented administrative software systems and the resulting lack of communication and information sharing. The first step on this endeavor was documenting the users' needs. To accomplish this, the Computing Services department, teamed with an external consultant, scheduled an entire week of one- and two-hour meetings with user departments. The agenda of these meetings was not only to document requirements for daily operations, but for the user communities to generate a 'wish list' of what would ideally aid them in their functions and the ultimate strategic goals of the University.

The information gleaned from this series of meetings was used to create a Request for Proposal (RFP) sent to 33 administrative software vendors. Of the 33, we received only nine legitimate responses. When the candidates were scored and weighted against the criteria outlined in the RFP, the Datatel Colleague and Benefactor systems emerged with the best scoring.

Implementation

The implementation process began with several basic assumptions. These assumptions were held as basic parameters for the entire process and directed all activities. The assumptions were:

There would be no significant alterations or enhancements to the original purchased system until at least one year of operations. The Datatel system was installed and initially implemented in a 'vanilla' fashion. This forced the departments to carefully review their current work processes thoroughly and jettison the unnecessary, unwanted, and inefficient. The primary goal of this directive was to disallow the corruption of the software to enable the current dysfunctional administrative processes.

All implementation activities would be governed by four cross-functional teams. (Appendix A) All significant operational decisions would be reviewed by team consent, with disputes to be arbitrated by the primary implementation team. The goal of this approach was twofold: first, we would be able to leverage the knowledge of many individuals. We felt this necessary in a system implementation of this scope. Secondly, each person involved in the implementation teams acquired a sense of ownership in the entire process, and expended the efforts necessary to ensure a successful conversion.

The existence of any 'sacred cows' would not be recognized. Every process of every department was to be documented and thoroughly analyzed by the appropriate team. Each member of each team had the authority to ask 'Why?' and any point and to challenge the inclusion of any part of any process. If the reason of existence for that activity or process could not be proven to the satisfaction of the team, it was slated for discontinuance.

Analysis Process

Teams documented each process utilizing various business process reengineering tools including process flow charting, time cycle analysis, activity-based costing, and Pareto analyses. The flow charts allowed all participating team members to graphically follow the flow and decision-making activities involved in a process and proved invaluable in identifying 'widows and orphans', or activities that led nowhere and added no value to the process as a whole. Time-cycle analysis and activity-based costing gave the ability to produce 'what-if' scenarios with each process. We answered may questions of "If we cut out this step, what effect would it have on the total time and/or cost of the entire process?" "If we could make this activity more efficient and save this much time, how much money could be saved?" It was only through answering these type of questions that a truly successful system migration could be achieved. It is only through examining each business process in light of the overall institutional strategic directions that the administrative platform for the future may be built.

The natural result of this intensive self-examination was the formulation of 'ideal' process maps. We constructed these ideal business processes with no regard to perceived constraints. We found that only through the denial of any barriers to progress may the most progress be realized. The goal processes were then documented and quantified for presentation to and persuasion of senior administrative decision makers, again utilizing the graphical tools described above. Examples of these charts and graphs are in **Appendix A**.

The New Era Begins

Upon nearing the end of the justification and politicking stage, the team began to realize results from our efforts. In several cases, departmental responsibilities were reassigned to those areas most suited to the tasks. Personnel were relocated to departments directly related to their actual job functions. Departmental reporting responsibilities were given to identified owners of the data in the user community. Graduation responsibilities evolved from a tri-departmental exercise in chaos to one department and one designated supervisor with ultimate responsibility. However, many bloody

battles were fought to achieve these gains -- some lost, some won. Listed below are some of the victories I felt we achieved, as well as the primary contributing factors to that success.

Class Scheduling

- Process steps were reduced from 31 to 15
- Process cycle time dropped from 42 days to 17-20 days
- Accuracy of communicated information rose dramatically

Factors of success: integration of Colleague software, real-time updating of student files

Student Registration

Registration completion time fell from approx. 90 minutes to approx. 35 minutes

Factors of success: flatter learning curve of Colleague system from standardized screens and functions throughout all Student System modules. This allows more personnel to be cross-trained on multiple process functions.

Institutional Reporting

Captures approximately 20% more institutional reporting and student retention data

Factors of success: integration of all Student System modules from Admissions Prospects to Graduation Processor, extensive student demographics data collection capabilities, and very extensive ad hoc query capabilities

Decentralized Purchasing

Shifted responsibility of budget management to proper points of user responsibility, giving designated departmental budget officers accountability, control of all departmental funds, and detailed analysis and reporting tools

Factor of success: highly developed budgeting system relying of a budget responsibility tree with adequate internal security and allocation controls

Reduced Workloads

Check request percentages of total expense report submissions fell from approximately 95% of all purchasing traffic to less than 20%. This allowed each purchasing officer to reclaim 12 hours per week, with each senior budget officer reclaiming 3-5 hours per week.

Factors of success: again, capabilities of budgeting system allowing pre-authorized purchasing levels for budget officers, tracking of account encumbrances, and detailed reporting capabilities

Qualitative Benefits

- Greater trust and teamwork generated between administrators, staff, and faculty
- An infinitely greater level of communication between all administrative departments and key personnel

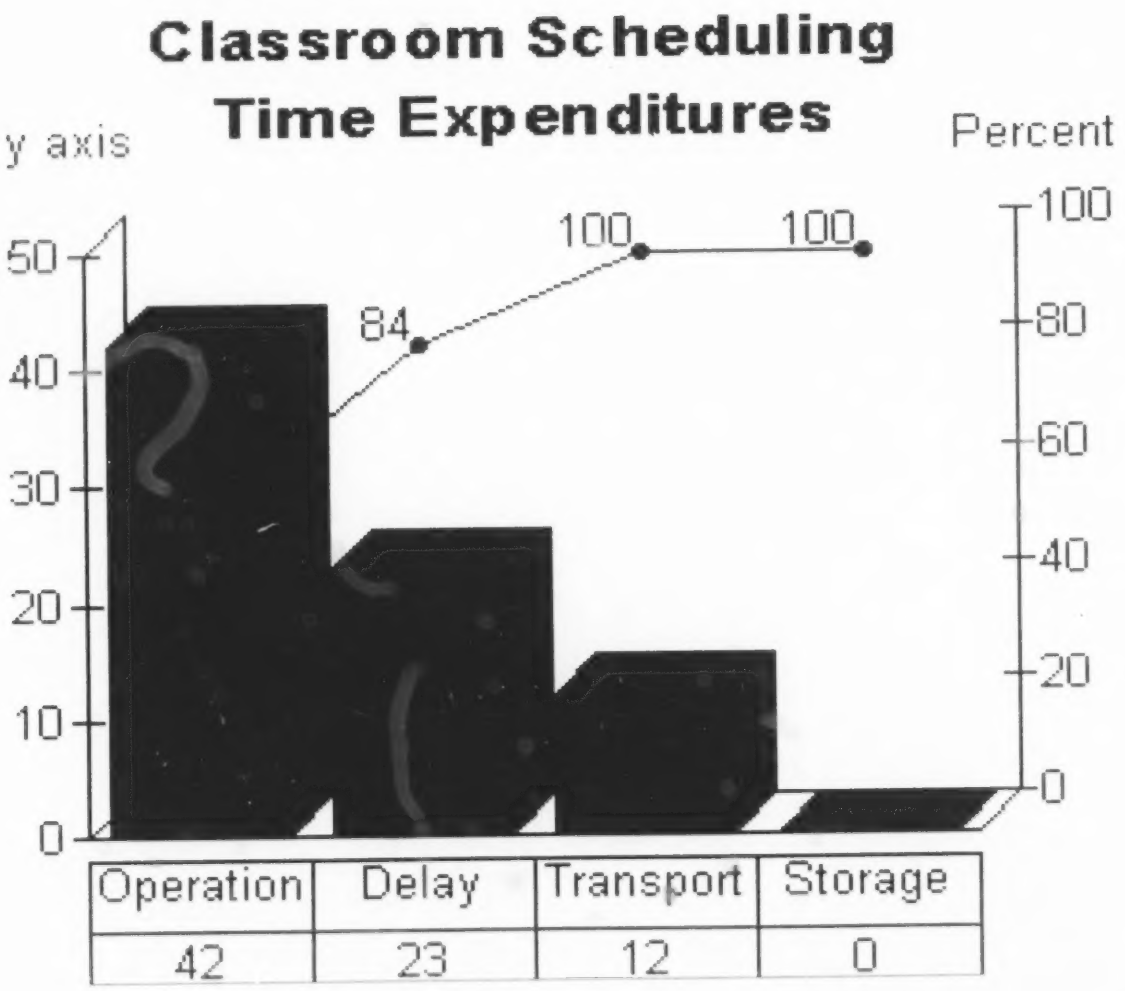
Factors of success: the teamwork approach used in the implementation process

The entire implementation process, while probably never labeled complete, is a success in any estimation. The benefits derived from taking a truly team-oriented approach to product selection and implementation will never be lost. As long as this administrative system, both software and people, functions, continued progress toward the institutional strategic goals is possible. The only barriers to continued advancement are ourselves, for the tools and infrastructure are there to be built upon.

> **"We trained hard... but it seemed that every time we were beginning to form into teams we would be reorganized... I was to learn later in left that we tend to meet any new situation by reorganization... and a wonderful method it can be for creating the illusion of progress while producing confusion, inefficiency, and demoralization."**
>
> **-- Petronious Arbitor, 210 B.C.**

APPENDIX A

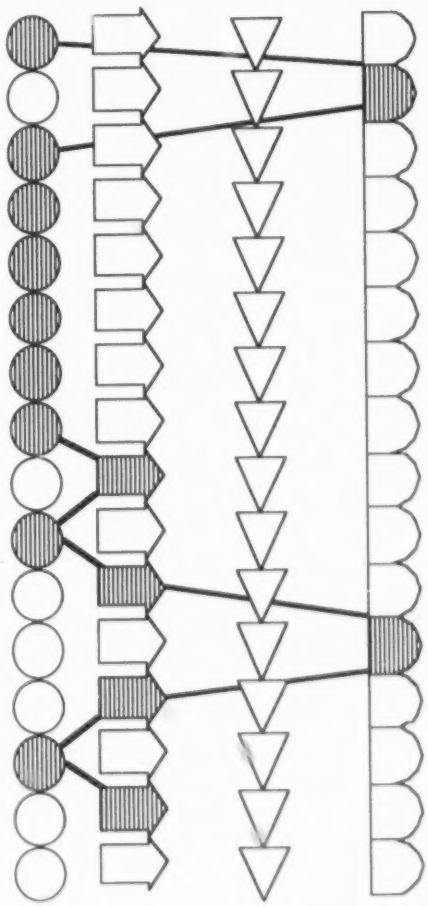
PARETO CHART EXAMPLE



Operation	Delay	Transport	Storage
42	23	12	0

PROCESS STEP CHART EXAMPLE - CLASSROOM SCHEDULING PROCESS

1	Colleges input tentative course schedul
2	Colleges request extension site course:
3	Extension site coordinators compile required cours
4	Extension site coordinators input required course
5	Colleges assign faculty to course
6.	Dean proof courses online
7	Deans make course changes online
8	Room assignments made online
9	Communications downloads schedule into DTF
10	Communications reformats for final deliver
11	Communications sends deliverable to deans
12	Deans proof final deliverable
13	Deans send changes to Communications
14	Communications inputs changes into DTP
15	Final copy sent to printer
16	



Computer Security

Questions to Ask .... Questions that Need Answers

Louise M. Schulden
Cornell University
Ithaca, NY

Current technology is putting information and computing into everyone's hands. Even Elementary school students are getting access to the Internet and surfing the net as soon as they develop reading skills. But can or should everything be available to everyone? Of course, the answer is "NO". Can it be secured in the current environment? That depends on your definition of "secured".

This paper looks at the information and services higher education institutions typically deal with and identifies the risks and exposures the current computing environment presents.

Introduction

Higher education is facing more competition, more discriminating customers, and less money. Controlling for every possible risk/exposure is not feasible and not in the best interest of our institutions. What is more important is that the risks and exposures are studied by the technical people and that the costs and benefits of eliminating the risks and exposures are presented to the institution's management and strategic planners for a decision on acceptable risk. Risks and exposures vary depending on the data (staff salary vs. student grades), the business application (writing payroll checks vs. admitting students), the computing environment (mainframe vs. client server), and communications (manual vs. electronic). In some cases, the law defines the security need. In other cases, it is a matter of politics and public relations. Sometimes it is even a matter of competitive advantage in an ever increasing competitive market. Security is not absolute. The best defense is knowing what your institution's risks and exposures are, how to minimize them, and which exposures you are willing to live with.

Computer Security means protecting a computer system against internal failure, human error, attack, and natural catastrophe. The goal is to prevent improper disclosure, modification, or destruction of information or deny service through the use of technological safeguards and managerial procedures. Security and control are a part of the entire computing environment. Security must utilize resources effectively and simultaneously minimize unnecessary interference with business goals, competitive performance, and the user's utility.

Security is a trade-off. The institution's managers and strategic planners must weigh total control and its costs/benefits against an acceptable level of risk. The institution's technical, business, legal and audit professionals can provide information to help management come to an informed decision.

Trends Increasing Risks

The following computing trends are presenting our institutions with incredible opportunities, but at the same time are increasing risks resulting in costly exposures.

The *decentralization* of hardware, software, data, computing personnel, and even technological decision making is evident in most organizations. With this, most organizations face a multiplicity of platforms and software. There is more to control, more to know, and in some cases it is hard to know what or where it is. There are users creating adhoc reports without controls resulting in duplication of effort and unreliable reports. The increased chance of misapplication of technical control features or lack of controls support by users increases the potential for operating errors and mistakes.

Microcomputing has become commonplace. Originally, microcomputers were used mostly to complement mainframe processing, i.e. a downloaded spreadsheet enabling further data manipulation. Now it is often the platform of choice for institutionally important processing. Unfortunately, the microcomputer environment is still far less secure and standards such as disaster recovery and software change procedures are not as diligently followed as its mainframe predecessor.

Communication and the Internet have revolutionized computing by *opening up access* to the world. Many of our institutions are connected to the Internet. There is more and more reliance upon this information and the communication vehicles computers provide. Many of us base decisions on information we obtained from listservers, bulletin boards, and electronic colleagues (E-mail).

More and more business authorizations and approvals are being conducted entirely over electronic media. Often signatures are only an electronic identifier stored in a data file. *Electronic approvals* are fast, easy and efficient, but to prevent fraud and to stand-up to auditor scrutiny proper controls are imperative.

Many institutions are *outsourcing* some or all of their computing. Many institutions have discontinued in-house systems development in favor of purchased system software. This can give the institution a false sense of security. Even though it is a vendor package your institution is still responsible to ensure that the system has proper controls and is properly implemented within your institution. Most outsource companies and some software package vendors have had their product/service audited. They should be able to provide you with a SAS-70 document citing control weaknesses.

The *technology is changing fast.*. Often with a new technology the security controls come later. In addition to a lack of security mechanisms, there are exposures created when staff are poorly trained and not equipped to properly implement or use the product.

Students, our single largest customer, grew-up with this technology and are comfortable with it. They are also very entrepreneurial and actively explore ways to exploit the technology made available to them. It is important that they understand the responsibilities that go along with the use of those resources.

Finally, many institutions are faced with *decreasing funds* and are *downsizing* their operations, particularly their administrative staff. Technology is being looked at to provide the means to accomplish the teaching and research missions of our institutions with less. Segregation of duties will not be possible as a control point, and computers will be relied upon to replace some of the current manual checks and balances. There will also be less IT staff. The industry standard for workstation support is recommended at 1 staff to 50 workstations. At Cornell that number varies from 1:100 to 1:200. Short-cuts are taken. Security administration, and LAN and workstation monitoring suffers. With downsizing and budget cuts comes a decrease in commitment to maintenance, system upgrades, and controls. Doing more with less often results in bypassing controls and security measures to get more work done.

Security , Controls, and Exposures

What needs protecting and why? Data needs protecting. Some data is protected by law. Our institutions have a responsibility due to 1) State/Federal/Agency Regulations and Requirements and 2) Laws protecting individuals such as FERPA, Privacy, and Labor laws. Compliance with regulations is increasingly important with research moneys becoming more scarce and indirect cost rates being scrutinized. Accounting and Human Resource information needs protection from fraudulent tampering. In other cases, security may be politically desirable.

Software Applications must be well controlled to ensure the institution's computer systems provide reliable information. Hardware, System Software, and data are valuable assets that must be secured and controlled to prevent tampering and guarantee continuing operations.

Finally, there is the misuse of the computing resources themselves. It may be the abuse of the institution's E-mail system or the setting up of a commercial web page on your university's network.

Exposures come in many forms and all can result in loss or harm to the institution. Erroneous recordkeeping, unmaintainable applications, or business interruptions can compromise the integrity of data. With decentralization and the move to smaller, more portable platforms, finding what needs protecting and determining whether there are sufficient controls is becoming more difficult. The key is to identify mission critical operations and the computing they use. Proper controls reduce institutional inefficiencies that would exist if for no other reason than the cost and time that goes into fraud investigations or dealing with a political/public relations problem.

The penalties include:

1) Adverse publicity or loss of reputation,
2) Disruption of service,
3) Downtime: delay: interim operation: recovery,
4) Fraud or embezzlement,
5) Future business or funding losses,
6) Investigations,
7) Litigation,
8) Loss of confidentiality,
9) Loss of goods,
10) Loss of money,
11) Loss of opportunities,
12) Loss of system integrity,
13) Misuse of resources, and
14) Staff disciplinary action.

Where is the Threat Coming From? Children are curious about using the computers...often they come into our university networks using their parents' or a friends' network logon. Hackers break in for the intellectual stimulation or the fun of it. Sometimes they find a logon without a password or one that has an easy password to guess. Enterprising students see the use (abuse) of the computer and network resources as their right simply because they are students at our institutions. Disgruntled employees are a possibility, but usually employee's are just using university resources for their own personal uses. What enables the abuse to occur is sloppy security administration, insufficient computing use and acquisition guidelines or methodology, insufficient or poorly communicated university policies, and insufficient controls over resources. Interestingly enough, hackers are not the number one threat.

Information Security Threats ***

Accidents and Errors	55%
Employee Dishonesty	15%
Fire, Flood, Earthquakes, Natural Disasters	15%
Employee Revenge	10%
Hackers	5%

***Commitment to Security, The Second Statistical Report of the National Center for Computer Crime Data (Santa Cruz, CA: National Center for Computer Crime Data, 1989)

Risks and A Sample Risk Analysis

Risk is the probability that a particular threat will exploit a particular vulnerability of the system. A *risk analysis* is a formal examination of an organization's information resources, controls, and vulnerabilities in both manual and automated systems. A *risk*

assessment identifies and evaluates the types of risks, their probability of occurrence, and their potential adverse impact for an automated information system.

The goal is to manage the risk by identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost-benefit analysis, and an overall system security review as well as the selection, implementation, testing and evaluation of safeguards. The result should be the institution operating at a level of risk they are comfortable with, an acceptable risk. Management's acceptance of a level of risk must be based on empirical data and supportive technical opinion that the overall risk is understood and that the controls placed on the asset or environment will lower the potential for loss.

Recently Cornell implemented two applications: Employee Essentials (A human resource inquiry client server application) and Faculty Advisor which was made available through the web. Security and control is relative. Cornell does not run encrypted communications, so for years mainframe passwords have been flying unprotected across our network. Consequently, the use of client server and web technologies coupled with Kerberos or Sidecar, a ticket granting application for authorization and authentication (developed at Cornell) though not full-proof is an improvement. What is desirable when any new technology is introduced is a technical identification of the exposures and then for the technical, the auditing, the legal, and the business minds of an institution to identify the risks. Armed with the information, the leaders of the institution must decide whether the risks are worth it.

Risks are the potential for loss, best expressed as the answer to four questions:

* What could happen? (What is the threat?)
* How bad could it be? (What is the consequence?)
* How often might it happen? (What is the frequency?)
* How certain are the answers to the first three questions? (What is the degree of confidence?)

What follows is an excerpt from a risk analysis performed by Cornell Information Technology and Internal Audit for the Faculty Advisor Application recently put into production at Cornell.

Point of Exposures for Faculty Advisor

The key control points for client/server applications at Cornell are:

1) The authentication and authorization servers,
2) The communications media/mechanisms,
3) The client machine,
4) The user security habits, and
5) The application database server.

Risk 1: Physical Assault on the equipment. The equipment of concern under these circumstances are the kerberos servers that are providing client authentication, the application servers providing client authorization, and to a lesser degree the routers. These servers are currently in the machine room. If you could get access to them:

1) You could avoid all authentication and authorization checking and access any client server application of interest.
2) You could modify data that you should not.
3) You could damage the security databases cutting off services.

Control in Place or Compensating Control: As already stated the servers are in the machine room that is under limited access. Access to the room requires an access card which produces an audit trail of those who have entered the room. One could lock the machines up further, but operators do need access to them if for some reason they need to be rebooted.

Action Item: None.

Risk 2: Telenet Assault on the server from an idle session. If someone has left the computer session idle an individual could telenet to that machine and use that machine's access to gain access to the servers and control the data acquisition system from the idle machine. This would result with the hacker having full access to whatever the initiated session they teleneted to had.

Control in Place or Compensating Control: To do this the hacker would have to know a IP address and query that address during a time of idleness. The probability of this is low.

Action Item: None

Risk 3: Disaster Recovery and Backups on key security servers. Currently there are no formal action plans or off-site tape backups for the kerberos authentication server.

Control in Place or Compensating Control: The fileservers are backed up so the data would be available as long as the tapes are accessible and not damaged.

Action Item: Define a disaster recovery plan and make arrangements for off-site backup tape storage.

Risk 4: The security servers are on a commonly used net in CIT. This makes them an easy target for sniffing the lines from within the CCC building. With that they could find out the server's supervisor password and login directly to the security servers.

Control in Place or Compensating Control: Monitor logins to the server. Investigate unusual activity.

Action Item: Put the machine room on a separate net from the rest of CIT.

Risk 5 : IP Spoofing.

Control in Place or Compensating Control: None

Action Item: Do IP check.

Risk 6 : Passwords passing in clear text gives access to anyone with a sniffer on the net.

Control in Place or Compensating Control: Kerborize application or use Sidecar.

Action Item: Mandate client/server application guidelines to enforce proper use of security mechanisms.

Risk 7: Client infected with a Trojan Horse.

Control in Place or Compensating Control: None

Action Item: User education and security guidelines/awareness. The need to logout and reboot to insure idle machines were not tampered with. Logging out when application not in use.

Summary of Most Possible Concerns

Individuals getting access to information they should not and using that information inappropriately, such as student grades, social security numbers, sensitive personnel information. This could result in public embarrassment for the institution and privacy litigation or failure to comply with FERPA. Our best protection here is to perform and document a yearly survey of practices on other campuses to make sure we follow an "ordinary standard of care" and are not "deemed negligent" in our handling of sensitive information.

The technical group has added many more risks to the list. The analysis broke the application's exposures down by category: risks due to the application, the use of the network, the use of the web server, etc. In addition, a summary of concerns political, legal, audit, public relations specific to that application's information is being developed. This is a work in progress, which I doubt will ever be complete, but has assisted in the thought process that needs be part of new system endeavors. In addition, it should be noted several of the action items have already been addressed.

Risk Analysis 2: Network and FileServer Security

Identification of risks and exposures to the institution need to be done at all levels. From large applications serving the entire campus community to local office applications. Even in the audit office, you have to ask how secure is data on the audit office fileserver. The server is on a Novell network connected to the Cornell backbone with a dial-in capability. It was discussed that the security risks might justify taking the LAN off the backbone and turning off the dial-in modem. The wealth of information that comes to audit via the network from the university systems and the Internet and the ability to work in NYC on documents in Ithaca make going back to that isolated existence inconceivable. We determined though almost all our work is confidential, only the fraud and irregularity documents would present an unacceptable level of risk if they became available. The solution was a policy that all fraud and irregularity documents would be stored on floppies in locked cabinets.

Determining What Has to Be Secure - Data Security

The evolution of data processing from mainframes to distributed processing has put the greatest strain on the attempts to control security from a centralized location point. Distributed processing gives users control over their data processing and to a certain extent responsibility for protecting and securing their own data.

Information must be protected if:

Its disclosure could cause harm to an individual.
Its disclosure could cause embarrassment or loss to the institution.
Its alteration could result in financial loss or incorrect management decisions.
Its destruction could cause an interruption in critical organization functions.

Historically at Cornell, every piece of data was secured by default, unless otherwise specified. This is impractical from an administration point of view, and undesirable. The university works on information. Now Cornell is reevaluating the securing of data. A data administration function has been created, data stewards or custodians have been define, and the question is being asked is there a good reason for securing the data. The data stewards are entrusted to provide proper protection, maintenance, and usage control of the information and maintaining information utility and availability as well as ensuring authenticity and integrity. They are the institutional person most familiar with the use of the data and the legal and political implications for safeguarding it.

Data security requires: 1) classifying the data, 2) determining the types of security control required, 3) accessing the efficacy of existing safeguards, 4) identifying necessary additions and improvements in security measures, 5) determining the availability of resources, 6) determining the level of security coverage needed, and 8) selecting the appropriate security techniques.

Securing Personal Data

The right of privacy an individual's right to determine what personal information can be communicated, and to whom. Privacy is not a constitutional right. Privacy rights have largely developed in the twentieth century, as a mixture of state common law, federal and state statutes, and constitutional law. As a general rule, the courts do not like to get involved in workplace privacy issues. Traditionally, employers, have been allowed great leeway to protect their business by almost any means not clearly illegal. Various cases, both state and federal, have upheld the right of employers to search desks, lockers, file cabinets, and E-mail without a search warrant. Though there are legitimate reasons for companies to do such searches, people do not give up all privacy expectations simply by coming to work.

Under the standard of due care, organizations have a duty to provide for information security. The standard of due care relates back to what the reasonable and prudent person would do in similar circumstances. If a reasonable and prudent person would have foreseen the threat and placed a known countermeasure in place regardless of what the current industry practices are, that may be the context in which a system's negligence will be judged. If managers fail to take actions to make their information systems reasonably secure and as a result someone suffers damages when those systems are penetrated, the organization may be sued.

Information security is still largely an unknown entity to most people, including lawyers. The exact duty with respect to confidentiality, integrity, and availability is still evolving in the courts. Consequently, attorneys are a valuable addition to any information security team. Cornell's Information Technologies Division has recently added a lawyer to their staff. There are several benefits to involving attorneys. They may/can determine that the review findings should be protected under the attorney-client privilege act. They can assist in the interpretations of copyright laws or licensing agreement. And corrective actions recommended by a review team may require legal direction. As a member of an information security team they can assist in the identification of foreseeable threats and countermeasures for those threats, identify standards of due care and the organizational duties to users (including those required by statue), and identify countermeasures for threats, according to what a reasonable and prudent person in similar circumstances would implement.

Securing Student Data

The Family Educational Rights and Privacy Act of 1974 (FERPA) requires educational institutions in very specific ways to ensure the confidentiality of student information. Briefly, it prohibits the posting or disclosure without the student's consent of the following information: 1) student social security number, 2) student identification number, 3) courses elected, 4) grades earned, 5) grade point averages, 6) class rank, 7) date of birth, 8) place of birth, 9) home telephone listing, 10) academic and disciplinary actions, 11) the most recent student educational records from the previous educational agency or institution, 12) financial arrangements between the student and the institution, and 13) any other education record containing personally identifiable information.

Application and System Integration Controls

Business Applications must be secure to insure only authorized proper transactions occur. The new technologies such as local area networks (LANs), client/servers, and distributed computer environments increase the complexity and level of challenge for controlling the computing environment.

Three level of controls are required: 1) General Business, 2) Application, and 3) Project . General Business Controls include development team qualifications, business reasons for the integration, business resumption, change controls, network controls, and access controls. Application Controls include input edit controls, communication controls, documentation controls, user controls, acceptance testing controls, processing controls, and output controls. Project controls include budgets, schedules, performance measures, and project management.

Policies and Guidelines

Computing is a fluid entity but without a container it just flows uncontrolled, unusable. Policies and Guidelines are the structure that contains it. Policies communicate what is acceptable. Guidelines are examples how a policy might be applied to a specific situation. An outline or checklist of detailed procedures recommended to satisfy a policy. In many cases, policies and guidelines are written after the fact. It is important we anticipate the needs and exposures of the future. In many cases we could look to existing policies for guidance. For example, if I call out-of-town friends from work, I must reimburse the university for the phone call. If I E-mail them instead, I still use the university's resource, but are currently under no obligation to reimburse for the personal use.

The availability and the use of computing and network resources is skyrocketing and our staff, faculty, and students need guidance on what are acceptable ways to use these resources. Recently Cornell had two different sets of enterprising students selling Web services using Cornell facilities. It was not clearly communicated to these students that using Cornell's network resources (a non-profit) for commercial endeavors was not acceptable. Policies and guidelines are being written to fill the gap. There is a network administrators group on campus, a maillist containing everyone identified as a departmental LAN administrators, and a LAN administrators manual. In this Cornell uniformly communicates to those responsible for the installation and maintenance of LAN on the Cornell backbone.

There are numerous areas that institutions should create policy to protect themselves, two come to mind immediately, E-mail and unauthorized microcomputer software. E-mail policy should clearly state 1) whether any messages of a personal nature are permitted on

university's E-mail system, 2) whether messages sent on the E-mail system are subject to examination, at any time, by management, 3) what actions will be taken if E-mail is improperly used.

Unauthorized microcomputer software policy should clearly informed employees of the company's position with respect to the practice of copying software. Every year, numerous software copyright infringement suits are filed. In 1991, the Software Publishers Association filed about two lawsuits a week around the country, seeking damages of $100,000 per violation plus attorney fees. (The National Law Journal (Dec 9, 1991)) Software copyright and licensing violations put an entire organization at risk of copyright violation litigation, adverse publicity, ethics degradation, unreliable software, loss of software support, and virus contamination.

Security Awareness

Most security breaches are caused by employees acting in ways that undermine security controls. Usually such action is not deliberate. With the widespread use of microcomputers, many security controls are manageable only by the employees themselves. A security awareness program should cover: 1) What should be protected. 2) What employee actions are required. 3) What employees should do if a problem is found. Each employee should know who is responsible for security investigations and should understand the role of internal auditors, the data security administrator, and anyone else involved in investigating a security problem. The controls are everyone's responsibility and concern, not just the computer professionals.

Employees are more likely to follow instruction regarding security precautions when they understand why security is important and controls are needed. The importance of controls should be reinforced by presenting situations they can relate to; users can quickly understand data vulnerabilities if they realize that there is a personal risk involved. For example, most microcomputer users appreciate the impact that the destruction of their hard disks would have on them.

Security Program Topics

Personal conduct
Password management
Physical access controls, Protecting diskettes, and securing equipment
Environmental controls
Information classification, storage, distribution, and disposal
Securing confidential information
Authorization and Authentication
Errors and Information Integrity-prevention, detection, and correction
Backups and Disaster recovery
Legal issues
Portable computers
Copyrights
Viruses

The top efforts on my list are disaster recovery, software piracy, password management, and quality assurance of custom-developed software (even spreadsheet formulas need to be controlled). Only by educating the faculty, staff, and students about the risks and their personal responsibility for preventing misuse of the institutional information and computing assets can you hope to be successful.

Final Topic: Passwords , Authentication, and Authorization

Passwords are problematic. They are too easily monitored, trapped, copied, and replayed over communication lines and on networks. Too often they are copied or written down. Often passwords are too simple and easily guessed. Frequently inadvertently they are disclosed when initially assigned or handed out. People shared passwords. Passwords can be learned by observing the user keystrokes or easily obtainable by decoy or deception. Hackers will trade passwords like baseball cards. And quite often, passwords are changed too infrequently (and too frequently changed back to the original). And yet passwords remain the foundation for much of our security.

With the increasing use of networks and of outside access to computer resources, the need for security has never been greater. Authentication is the keystone in a sound security program. Authentication is the act of verifying the identity of a station, originator, or individual to determine the right to access specific categories of information. Also a measure designed to protect against fraudulent transmission is by verifying the validity of a transmission, message, station, or originator. Based on knowledge of who the user is, we can control access, authorize the user privileges to perform functions and manipulate data, allow the use of encryption engines, and effectively hold the user accountable for his actions. Dynamic password technology, whether implemented in hardware or software is a secure, reliable way to obtain authentication.

Summary

Security is, above all, about people and a continuing commitment to secure and control the computing environment from people at all levels and in all parts of the organization. It is not cost-effective to implement more security procedures than a given environment requires. Risk analysis can help define realistic security requirements and therefore control the cost of security. A risk assessment methodology will define assets, review threats, identify security requirements, and select protective counter measures not only for the computer professional in the organization, but more importantly for the operational and executive management.

It is important to organize your institution for security by instituting security policies and standards and guidelines. Make sure your policies and procedures protect what you want/are required to protect. You will need baseline security controls, a basic set of controls that meet a minimum set of standards that should be in place in all properly run data centers, LANs, and workstations. It is useless for an organization to develop policies, however sound, if the technology is unable to support those policies. Laws against back robbery and theft would be meaningless if banks left money in the open with no guards, vaults, or alarms to protect it. A commitment to data security unsupported by necessary technological and administrative methods is worthless.

Most importantly your institution must have a commitment to meaningful data security. This can start with a security awareness program which covers what should be protected, what employee actions are required, and what employees should do if a problem is discovered. In all cases, the assignment of specific individual responsibility for information privacy and security and for everyone in the organization to accept personal responsibility and accountability is essential for success.

Lock the Door and Throw Away the Key?

. . . *If we cannot provide access to data, why collect it?*

Richard Pickett II
Data Administrator
Princeton University
Princeton NJ
pickett@princeton.edu

Darlene Quackenbush
Director
Information Technology Planning
James Madison University
Harrisonburg VA
quackedh@jmu.edu

Abstract

Megabytes, gigabytes, terabytes, and petabytes. Institutions of higher education continue to collect ever increasing amounts of data. The intriguing challenge is not so much collecting the information as in providing useful end-user access. As campus users acquire more powerful computers with easy-to-use interfaces, they have come to expect comparable ease of use and sophistication in their administrative applications, especially when it comes to gaining access to this data.

Providing such access to data raises numerous, interrelated issues: What is the impact on data integrity, security, and data administration? Such issues need to be considered, and institutions of higher education need to institute policies in order to encourage and sustain, effective use. In the end, if the information we collect is not accessible, then why collect it?

Introduction

In many cultures, storytellers have been responsible for accumulating and recalling local histories and information vital to the welfare of their audience. As the guardians of the community's information resources, storytellers have the important responsibility of passing information to the next generation. In a real sense, they are their culture's central database, retrieving and updating data as needed. This information transfer allows succeeding generations to manage their lives and their culture more effectively.

Organizations, including higher education, are becoming increasingly aware that their own "stories"; or, in this case, the data contained in various computer applications, are a strategic asset. Our organizations need the information for day-to-day operations as well as for long-term decision-making. A number of universities and colleges have been pioneers in this area, including Virginia Tech, University of Pennsylvania, Stanford, and University of Michigan. We are increasingly aware that the availability of information is essential in all aspects of the work environment.

Increasing volume of data

This data comes in new forms and delivery mechanisms including sound, picture and virtual reality presentations and from sources as close as the palmtop we are holding or as far away as a repository on the other side of the Internet. The electronic collection of information is relatively new in relationship to the age of many institutions. In the case of Princeton, we have a computerized "history" that represents less than one-tenth of our 250 year life as a university. During this relatively brief period we have accumulated more information than imaginable just 30 years ago. Since we must assume that this collection of information will only escalate, it is important to plan for the future.

In her CAUSE94 presentation, Building the 21st Century Mind, Jennifer James noted that individuals in our current information age have to assimilate 400 times more information than their Renaissance counterparts. To deal with this information overload, users have had to become data literate. Sources and uses of data must be known and understood by all who hope to cope in this age of information.

Greater technology awareness

Awareness of technology is fast becoming part of the societal norm, presenting technology managers with a clientele who is increasingly more demanding. Slow, cumbersome or unnecessarily restrictive systems are viewed with disdain. Technical decisions are open to increased scrutiny based on new levels of awareness and understanding. As a result of this increased technological awareness, new business and academic perspectives are being considered in the delivery of data. A key component of the increasing use of business

process reengineering (BPR) is technology. In fact, for BPR to succeed, technology must be creatively utilized.[1]

Impact of Distributed Information Sources

Before the advent of personal computers, the vast majority of an organization's electronic information was centrally managed, maintained, and secured. The historical mindset did not usually include distributed processing. As we all know, the advent of personal computers has permanently changed the way computer resources are distributed. When people discovered the power of computing that they could personally control there was an increasing desire to develop individual or departmental applications, often without consideration of the organization-wide impact. Traditional computing data centers were ill-equipped to manage, much less control, the proliferation of systems.

With this explosive growth in distributed computing, there was a concomitant increase in the number of isolated pockets of data. Shadow systems with financial, personnel, and student information proliferated. Duplicate information in these fragmented data stores was collected, stored, and analyzed. In many cases inconsistent information was separately supplied to decision-makers and the resulting lack of planning and coordination of distributed computing has become a hindrance rather than a facilitator of information exchange.[2]

The pendulum that represents the shift from totally centralized computing to fully distributed appears to be drifting back. That does not mean we are returning to a centrally controlled data center, but does represent a return to some centralized management of data -- but with improved access.

Needs and Benefits of Strategic Planning for Data Access

Changes in the technology environment are encouraging increased demands for data **A**ccuracy, **A**ccess, and **A**ccountability. Coincidentally, an even larger and inescapably complex array of pressures facing academic institutions is leading many to focus energy and resources on these "three A's" as a possible avenue to success. The result is that one of the university's most valuable assets, information, is moved up on the strategic planning agenda. What, then, does senior management want?

Data Accuracy

In a nutshell, what institutions want is confidence that the information asset is derived and managed to ensure its integrity and utility. Electronic information is increasingly utilized to make strategic decisions such as budget, enrollment forecasts, and faculty workload. Data that is accurate, complete and concocted according to the needs of the institution is a prized

[1] "Public Sector Reengineering," Government Technology, September 1995, pp. 30-31
[2] Wayne Rhodes, "Learning to Share," Beyond Computing, July 1995, pp. 48-49

delicacy. It is one best served in ample portions enriched by easy-to-use interfaces, on top of a rich complement of powerful data storage and manipulation tools and covered with a transparent glaze of safeguards to its continued quality. The appetite for complete, timely, and meaningful information from institutional data repositories seems insatiable.

Access to Information

Information has always had a very high strategic and tactical value. In order to remain competitive, and be cost-effective, organizations must develop a new paradigm regarding access to data. Institutions must realize that data is an important asset that needs to be managed along with other valuable resources.

Our new data access paradigm must reinforce that providing access is not only viewed as a very positive characteristic, but as an essential service. Access to information traditionally controlled by individual departments within organizations is often difficult. In some instances the concerns are that the information will be incorrectly interpreted, or security violated. Convincing those that currently have this stewardship that this sharing of information is important can be a challenging task.

Shared Accountability

Closely tied to the lines of authority is security. Maximizing legal and practical protection against computer theft, eavesdropping, data tampering, and system invasion while providing for statutory requirements, business demands, and easy access by authorized users demands finesse. Information security requires on-going attention and yet has the potential of deterring efforts toward efficient and open data access. Data access models must find a fulcrum on which to balance reasonable risk and functionality if they are to succeed.

This search for an appropriate alignment of the data access model presents interesting issues especially as computing has become more distributed. The redistribution of the data begs a redistribution of authority and responsibility. As people have become technically literate and demand, rightfully, access to information, they also need to accept the responsibility for proper access control. Particularly in client/server architectures, these lines of responsibility and authority are often difficult to construct and maintain.

External Pressures

As if these internal calls for data integrity and management, improved access to information, good information security, and intelligently designed data access schemes are not enough, external pressures of great magnitude must be considered. External pressures from state/federal agencies, legislatures and individual citizens and patrons more than ever before require academic institutions to collect and process accurate information. Accountability for funds, ability to report and forecast university activity, and maintain the overall viability of the institution is all empowered by intelligent use of data.

Sample Approaches

Princeton University

At Princeton we currently have a large number of sophisticated automated systems that support the business and academic functions. These systems vary from new client/server applications to programs that are approaching 25 years of age. As with many organizations, the computer application demands of our users often out-stripped the resources of the centralized software development staff and the legacy systems. As these users became more technically capable they developed satellite systems to fill some of their needs, often with their own set of information. These systems helped to answer some of the computing needs of the university but at the same time increased the fragmentation of information. This growth of distributed data stores, coupled with the lack of full data integration in the central applications, has made it difficult to obtain information.

To remedy this situation, Princeton has embarked on a plan to develop a strong "*infocentric*" architecture. This architecture will serve to break down the barriers that have prevented decision-makers, from students to executives, from having current information. This is being accomplished by the establishment of a data administration function and new directions in application development. There is a strong awareness on our campus that the sharing of information is an important factor in the future management of our institution. This concept is the basis for the mission of data administration, facilitating the utilization of information across organizational units.

One of the first projects to increase access to information is the creation of the Princeton Data Mall. This is the establishment of a multifunctional data warehouse, whose first customers will be the managers of academic departments. When conceptualizing this data resource we visualized a shopping mall, with a varied collection of data "stores", each with its own specialty, some overlap in product availability, ease of window shopping, extended hours of operation, but with a common location, and architecture.

James Madison University

James Madison University faced similar circumstances: aging central systems powered by non-relational, proprietary databases; an increasing number of distributed, and disjointed, spin-off systems; and no strategy to achieve long-term viability. JMU chose to act boldly to achieve greater information sharing. The current project not only replaces the Finance, Human Resources and Student Information systems, but also aims to provide an integrated source of information to which other systems can be joined. The Integrated Information System (IIS) project is in progress and will facilitate the sharing of information and provide new functionality across departments and systems.

At the foundation of this effort is a move to relational database (Oracle) storage and retrieval. To this is added a client/server processing model and easy-to-use data query and reporting tools supported by the application vendor (PeopleSoft). Most importantly, a conscientious effort is being made to craft new policies and practices which offer supportive access to information on behalf of the university.

Success Factors

Senior Management Support

Frequently it is stated that the support of the senior management of an organization is a very important aspect of any successful project. With regard to data access, this support is imperative to help break down barriers such as financial, ownership, and shared access hurdles.

User Involvement

While without doubt the support of the executives is crucial, it is the acceptance of the project by the staff that makes implementation a success. This is particularly true since the creation of new computer systems can place a heavy toil on the individuals involved.

The role of users in the management of information technology projects is increasing. A recent survey by Deloitte & Touche of Chief Information Officers indicates that a vast majority (96%) believes that users should either lead or work as a team with information professionals in managing projects.[3] In addition, integration of user input in the design, development, and implementation is essential. This integration increases the probability that these systems will meet the business needs of the institutions. This has been particularly important in the efforts that have been undertaken at both Princeton and James Madison University.

Data Administration

The basic concepts of effective data administration are not new. Before the advent of personal computers the data was centrally located and management was relatively simple. The advent of distributed computing and client/server architecture has complicated the situation, but the overriding goal of assuring accurate corporate information remains. While many large higher education institutions have established this functionality within their organizations, it is an important issue for all colleges and universities to address.

The establishment of data administration should be a very positive experience, one that can facilitate the utilization of information across the campus. This is a shared responsibility between the technologists and users of information requiring a coordinated effort to ensure access to accurate and timely data.

New Technologies and Methods

With the ever-increasing amounts of data that will be collected in the future, it is important that we continue to scan the horizon for new tools. Moreover, we must seek to provide additional functionality using our institutional data while seeking to involve new data providers and users.

---

[3] "Leading Trends in Information Services," Deloitte & Touche, 1995

In addition, we must find new ways to provide better service and greater value to our institution through well-planned information access and use.

Summary

Today, and probably for the foreseeable future, higher education is under increasing pressure to maximize the effectiveness of many resources, including data. Our ability to collect information has grown faster than our ability to distribute and understand it. To avoid making business decisions based upon incomplete, or even erroneous data, it is imperative that methods be developed to properly manage and distribute this resource.

The growing trend in distributed computing will require new paradigms in the delivery of electronic information. Data located in distributed information systems need to be evaluated for organization-wide impact. These islands of data have the potential to affect the effectiveness of managing information. As we manage these data stores information technology professionals must work closely with the potential users of information. Only through a mutual partnership will organizations be able to fully utilize the electronic stores of information.

Changing technology calls for constant reeducation. However, when access is considered, the education is not limited to learning new technical operations but also an understanding of needs across the university campus and a willingness to rethink one's role in university functions. "We've always done it that way", is out.